

EXHIBIT A

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK**

IN RE GOOGLE DIGITAL ADVERTISING
ANTITRUST LITIGATION

Case No. 1:21-md-3010 (PKC)

NOTICE OF ISSUANCE OF SUBPOENA

PLEASE TAKE NOTICE that, pursuant to Rule 34(c) and Rule 45 of the Federal Rules of Civil Procedure, the MDL Plaintiffs' Discovery Steering Committee in the above-captioned matter intend to arrange for service of the subpoena for documents for the following entity:

Subpoena Recipient

The State of Texas

The subpoena is attached to the email by which this notice is provided. The documents to be produced are described in Exhibit A.

DATED: April 26, 2024

Respectfully submitted,

/s/ Philip C. Korologos

Philip C. Korologos

pkorologos@bsflp.com

BOIES SCHILLER FLEXNER LLP

55 Hudson Yards, 20th Floor

New York, NY 10001

Telephone: (212) 446-2300

Jordan Elias

GIRARD SHARP LLP

601 California Street, Suite 1400

San Francisco, CA 94108

Telephone: 415.981.4800

jelias@girardsharp.com

Serina M. Vash

HERMAN JONES LLP

153 Central Avenue #131

Westfield, New Jersey 07090

Telephone: 404-504-6516

svash@hermanjones.com

*MDL Plaintiffs' Discovery Steering
Committee*

CERTIFICATE OF SERVICE

I hereby certify that on April 26, 2024, a true and correct copy of Notice of Issuance of Subpoena was served on all counsel of record via email.

Date: April 26, 2024

By: /s/ Philip C. Korologos
Philip C. Korologos



Philip C. Korologos
(212) 446-2390
pkorologos@bsfllp.com

April 26, 2024

The State of Texas

c/o Trevor Young
Office of the Attorney General, Antitrust Division
State of Texas
300 W. 15th Street
Austin, TX 78701
Trevor.Young@oag.texas.gov

c/o Zeke DeRose, III
The Lanier Law Firm
10940 W. Sam Houston Pkwy N.
Suite 100
Houston, TX 77064
Zeke.DeRose@LanierLawFirm.com

In re Google Digital Advertising Antitrust Litigation
No. 1:21-md-3010 (PKC) (S.D.N.Y.)

Dear Counsel:

I am counsel for plaintiff Genius Media Group Inc. and co-lead counsel for the Publisher Class in *In re Google Digital Publisher Antitrust Litigation*, No. 21-cv-7034 (PKC) (S.D.N.Y.), which has been consolidated into the above-captioned multi-district litigation. On behalf of the MDL Plaintiffs' Steering Committee in the above-captioned litigation, enclosed for service upon the State of Texas is a subpoena to produce documents.

Treatment of discovery materials in this litigation is governed by a Confidentiality Order and Order Regarding Discovery Procedure which have been entered by the Court. Copies of both orders are enclosed with this subpoena.

Please contact me should you have any questions.

Sincerely yours,

/s/ Philip C. Korologos
Philip C. Korologos

Enclosures.

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In re Google Digital Advertising Antitrust Litigation

Plaintiff

v.

Defendant

Civil Action No. 1:21-md-3010 (PKC) (S.D.N.Y)

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS
OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: State of Texas, attn: Office of the Attorney General, Antitrust Division

(Name of person to whom this subpoena is directed)

☒ **Production:** **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material: Described in the attached Exhibit A.

Place: Boies Schiller Flexner LLP
c/o Izaak Earnhardt, iearnhardt@bsflp.com
55 Hudson Yards, 20th Floor, New York, NY 10001

Date and Time:

05/17/2024 5:00 pm

☐ **Inspection of Premises:** **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:

Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 04/26/2024

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk

/s/ Philip C. Korologos

Attorney's signature

The name, address, e-mail address, and telephone number of the attorney representing (name of party) Genius Media Group, Inc. (n/k/a Medialab.AI Inc.), who issues or requests this subpoena, are:

On behalf of MDL Plaintiffs' Discovery Steering Committee: Philip C. Korologos, Boies Schiller Flexner LLP, 55 Hudson Yards, 20th Floor, New York, NY 10001; pkorologos@bsflp.com; (212) 446-2300

Notice to the person who issues or requests this subpoena

A notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 1:21-md-3010 (PKC) (S.D.N.Y)

PROOF OF SERVICE*(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)*

I received this subpoena for *(name of individual and title, if any)* _____
 on *(date)* _____.

☐ I served the subpoena by delivering a copy to the named person as follows: _____

_____ on *(date)* _____; or

☐ I returned the subpoena unexecuted because: _____

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also
 tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of
 \$ _____.

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)**(c) Place of Compliance.**

(1) For a Trial, Hearing, or Deposition. A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

- (A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or
- (B) within the state where the person resides, is employed, or regularly transacts business in person, if the person
 - (i) is a party or a party's officer; or
 - (ii) is commanded to attend a trial and would not incur substantial expense.

(2) For Other Discovery. A subpoena may command:

- (A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and
- (B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) Avoiding Undue Burden or Expense; Sanctions. A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) Command to Produce Materials or Permit Inspection.

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

- (i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.
- (ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) Quashing or Modifying a Subpoena.

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

- (i) fails to allow a reasonable time to comply;
- (ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);
- (iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or
- (iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

- (i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

- (i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and
- (ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) Producing Documents or Electronically Stored Information. These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) Claiming Privilege or Protection.

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

- (i) expressly make the claim; and
- (ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

Exhibit A to Subpoena

INSTRUCTIONS

1. In addition to the specific instructions set forth below, these requests incorporate the instructions set forth in Federal Rule of Civil Procedure 45 (“Federal Rules”), the Local Rules of the U.S. District Court for the Southern District of New York (“Local Rules”), the Stipulation and Order Regarding Discovery Procedure (“ESI Order”) (ECF No. 508), the Confidentiality Order (ECF No. 611-1; *see* ECF No. 685), and Pre-Trial Order No. 5 (“Scheduling Order”) (ECF No. 394), or the operative version of those Orders in place at the time production is made. Subject to a valid claim of privilege, please produce the entire document if any part of that document is responsive.

2. Please produce the Documents responsive to the numbered requests below that are in Your possession, custody, or control, including Documents in the possession of Your attorneys, accountants, consultants, or other agents.

3. Pursuant to Federal Rule 45(e)(1), documents must be produced either: (a) as they are kept in the usual course of business (in which case they must be produced in such fashion as to identify the department, branch, or office in whose possession the document was found or the server or central file in which it was found, and the address of each document’s custodian(s)), or (b) segregated as responsive to a specific request enumerated herein, with such specific request identified.

4. The terms defined below and in the individual requests for production and inspection are to be construed broadly to the fullest extent of their meaning in good faith effort to comply with the Federal Rules of Civil Procedure. Additionally,

- a. Terms not specifically defined are to be given their ordinary meaning as you understand them to be used in the trade or industry;
- b. The use of a verb in any tense, mood, or voice shall be construed as the use of the verb in all other tenses, moods, or voices, whenever necessary, to bring within the scope of any Request all information that might otherwise be construed to be

outside its scope;

- c. The use of the singular form of any word includes the plural and vice versa;
- d. Words in the masculine, feminine, or neutral gender shall include each of the other genders;
- e. The connectives “and” and “or” shall be construed either disjunctively or conjunctively as necessary to bring within the scope of the Request all responses that might otherwise be construed to be outside of its scope;
- f. The terms “all,” “any,” and “each” shall each be construed as encompassing any and all.

5. All documents are to be produced in full. If any portion of any document is responsive to any request, a legible version of the entire document must be produced, together with all non-identical copies, versions, and drafts of that document, including all attachments and enclosures.

6. You must retain all of the original documents for inspection or copying throughout the pendency of this Action, any appeal(s), and any related proceedings.

7. You must produce all documents and associated metadata according to the Federal Rules, Local Rules, and, when entered, the governing ESI Order for this Action. Provide instructions and all other materials necessary to use or interpret Your data compilations, such as a data dictionary, with Your production.

8. Data and materials that are stored electronically or in machine-readable form should be produced in electronic form with sufficient information to allow counsel to readily access or read such data or materials. None of the definitions or requests set forth herein shall be construed as an admission relating to the existence of any evidence, to the relevance or admissibility of any evidence, or to the truth or accuracy of any statement or characterization in the Definitions or the requests.

9. If you object to all or any portion of any of the below requests, you must identify the objectionable request or portion thereof, and the nature and basis of the objection.

Notwithstanding any objection to any portion of any Request, you must produce all documents and information to which such objection does not apply.

10. If any document responsive to a particular Request no longer exists for reasons other than Your document retention policy, describe the circumstances under which it was lost or destroyed, describe the information lost or destroyed, list the Request to which it was responsive, and list persons with knowledge of the document.

11. If you are unable to produce a document that is responsive to a Request, describe the document, state why it cannot be produced and, if applicable, state the whereabouts of such document when last in your possession, custody, or control.

12. If there are no documents or information responsive to all or any portion of any request, so state in writing.

13. Other than redactions of privileged information, documents are to be produced in full. If any requested document cannot be produced in full, or if you withhold production of any document or portion of any document responsive to these requests based upon any privilege, protection, or immunity, produce it to the extent possible and provide the privilege log information set forth in the governing ESI Order.

14. Unless otherwise stated, the requests seek documents and data from January 1, 2013 to the present (the “Relevant Time Period”). Because these requests are ongoing, please promptly produce any document discovered or obtained after service of these requests.

15. If any document responsive to a request exists or existed but cannot be located, please state with particularity the efforts made to locate the document and the specific reason for its destruction or unavailability.

DEFINITIONS

1. To the extent the terms defined below are used in the Requests, they should be construed broadly to the fullest extent of their meaning in a good-faith effort to comply with the Federal Rules and the Local Rules. These Definitions are provided solely for the purposes of this Subpoena.

2. The term “**document**” shall have the meaning provided in Local Rule 26.3, namely, that the term shall be synonymous in meaning and equal in scope to the usage of the phrase “documents or electronically stored information” in Federal Rule 34(a)(1)(A). A draft or non-identical copy is a separate document within the meaning of this term.

3. The term “**Google**” shall mean Google LLC, any current or former parents, subsidiaries, affiliates, divisions, predecessors, officers, directors, employees, agents or representatives, and any other person acting on their behalf.

4. The term “**includes**” shall mean “includes, but not limited to”; and “**including**” shall mean including but not limited to.

5. The term “**MDL Action**” shall mean *In re Google Digital Advertising Antitrust Litigation*, No. 21-md-3010 (PKC) pending in the United States District Court for the Southern District of New York.

6. The term “**MDL Plaintiffs**” shall mean all plaintiffs in the actions consolidated for pre-trial proceedings in the MDL Action.

7. The term “**Texas Action**” shall mean *Texas v. Google, LLC*, No. 4:20-cv-00957-SDJ filed in the United States District Court for the Eastern District of Texas.

8. The terms “**You**” or “**Your**” refer to the State of Texas as the Plaintiff in case *Texas v. Google, LLC*, No. 4:20-cv-00957-SDJ filed in the United States District Court for the Eastern District of Texas.

REQUESTS

1. Deposition notices served by You or served by Google in the Texas Action, whether served upon You, Google, or a non-party after March 1, 2024.

2. Unredacted copies of all sealed filings made in the Texas Action made by you or Google, excluding sealed filings relating to discovery from non-parties or filings sealed because of the presence of materials which MDL Plaintiffs are prohibited from receiving by an order in the MDL Action or Texas Action.

3. All deposition transcripts and associated documents from all depositions of current

Google employees, former Google employees, or witnesses designated by Google pursuant to Rule 30(b)(6) taken in the Texas Action after March 1, 2024, including, for each deposition, (1) unredacted copies of all deposition transcripts in PDF and available native text formats (*e.g.*, .ptx, .txt); (2) all video recordings of the deposition; (3) all marked versions of exhibits; and (4) all errata sheets. Documents produced pursuant to this request may be transmitted in the form that they are received from the court reporter.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

| | | |
|----------------------------------------------------------|--|-----------------------------------|
| <i>In re Google Digital Advertising Antitrust Litig.</i> | | Civil Action No. 21-MD-3010 (PKC) |
|----------------------------------------------------------|--|-----------------------------------|

MODIFIED CONFIDENTIALITY ORDER

In the interests of: (i) ensuring efficient and prompt resolution of these Actions; (ii) discovery by the Parties litigating these Actions; and (iii) protecting certain information from improper disclosure or use, the Court enters the following Confidentiality Order. This Order supersedes all protective orders or confidentiality orders previously entered in any of the Actions, as defined below in Paragraph 1(a).¹

The Court, upon good cause shown and pursuant to Fed. R. Civ. P. 26(c)(1), ORDERS as follows:

A. Definitions

1. As used herein:

(a) “Actions” means collectively the actions centralized by the Judicial Panel on Multidistrict Litigation under the caption *In re Google Digital Advertising Antitrust Litig.*, No. 21-MD-3010 (PKC) (S.D.N.Y.), as well as any additional actions subsequently transferred and/or

¹ For the avoidance of doubt, the Agreed Protective Order between Google and the Office of the Attorney General of Texas, entered in Texas state court on February 20, 2020 (the “Texas OAG Order”), *Google v. Paxton*, No. D-1-GN-19-007654 (261st Dist. Ct., Travis County, Tex., Feb. 21, 2020), and the Confidentiality Agreement entered into In The Matter of The Multistate Investigation of Alphabet Inc., between Google and various states, including State Plaintiffs, dated February 20, 2020 (the “Multistate Confidentiality Agreement”) are superseded by this Order, as to any State Plaintiff. For all other states which are not State Plaintiffs, the Multistate Confidentiality Agreement remains in full force and effect.

centralized with these Actions, including any related discovery, pretrial, trial, post-trial, or appellate proceedings. The term Action means an individual action within the Actions. For the avoidance of doubt, “Actions” excludes pre-suit investigations by State Plaintiffs.

(b) “Confidential Information” or “Confidential” means information (regardless of how it is generated, stored or maintained) or tangible things that constitute a trade secret or other non-public confidential financial, technical, research, sales, marketing, development, or commercial information and that have been so designated, or any Document, transcript, or other material containing such information that has not been published or otherwise made publicly available.² In addition, a Designating Party may designate as Confidential any information or items made publicly available in violation of a court order to keep such information confidential, that the Designating Party believes should receive Confidential treatment. Confidential Information includes (i) information copied or extracted, summarized or compiled from Confidential Information, and (ii) testimony, conversations, or presentations by Parties or their Counsel that reveal Confidential Information.

(c) “Competitive Decision-Making” means the action or process of making a business decision or resolving a non-legal question relating to a competitor, potential competitor, customer, or distribution partner regarding contracts, marketing, pricing, product, service development or design, product, or service offering, research and development, mergers and acquisitions, or licensing, acquisition, funding or enforcement of intellectual property. It does not include legal advice provided in connection with litigation, potential litigation, or regulatory

² For the avoidance of doubt, the Receiving Party’s belief that material designated as Confidential does not meet this standard shall not deprive such material of the protections afforded to Confidential Information. Any challenge to a designation is subject to Paragraph 13.

matters, nor does it include work performed as part of a trial team or to keep management advised on the progress or status of litigation, potential litigation, or regulatory matters.

(d) “Defendant” means any party named as a defendant in any of the Actions, including their parents, divisions, subsidiaries, affiliates, partnerships and joint ventures, and all directors, officers, employees, agents (including counsel), and representatives of the foregoing.

(e) “Designated In-House Counsel” means up to four In-House Counsel designated by a Defendant or Plaintiff who may be authorized to access Highly Confidential Information pursuant to Paragraph 19 of this Order.

(f) “Disclosed” means shown, divulged, revealed, produced, described, transmitted or otherwise communicated, in whole or in part.

(g) “Document” means any document or electronically stored information, as the term is used in Fed. R. Civ. P. 34(a).

(h) “Highly Confidential Information” or “Highly Confidential,” as defined herein, shall only include information that, if disclosed publicly or to a Party, is likely to cause the Producing Party material and significant competitive or commercial harm, and that has been so designated.³ Subject to the foregoing, Highly Confidential Information may include trade secrets, including algorithms and Source Code; non-public, commercially sensitive customer lists; non-public financial, marketing, or strategic business planning information; current or future non-public information regarding prices, costs, or margins; information relating to research, development testing of, or plans for existing or proposed future products; evaluation of the strengths and vulnerabilities of a Protected Person’s product offerings, including non-public

³ For the avoidance of doubt, the Receiving Party’s belief that material designated as Highly Confidential does not meet this standard shall not deprive such material of the protections afforded to Highly Confidential Information. Any challenge to a designation is subject to Paragraph 13.

pricing and cost information; confidential contractual terms, proposed contractual terms, or negotiating positions (including internal deliberations about negotiating positions); information relating to pending or abandoned patent applications that have not been made available to the public; personnel files; sensitive personally identifiable information; and communications that disclose any Highly Confidential Information. Highly Confidential Information includes (i) information copied or extracted, summarized or compiled from Highly Confidential Information, and (ii) testimony, conversations, or presentations by Parties or their Counsel that would reveal Highly Confidential Information. A Designating Party may designate as Highly Confidential any information or items made publicly available in violation of a court order to keep such information confidential, that the Designating Party believes should receive Highly Confidential treatment. In addition, if a Protected Person (i) has produced Investigation Materials or (ii) is required by subpoena or court order to produce information that would cause it material and significant competitive or commercial harm, but that information does not specifically fall into one of the categories of information listed in this paragraph, upon a compelling showing, it may seek a court order that such information is Highly Confidential. If a motion is made pursuant to this paragraph and is related to a subpoena or court order, it must be filed no later than the due date to respond to the subpoena or court order. If a Protected Person seeks additional protection pursuant to this paragraph from the Court, the materials for which additional protection has been sought will not be provided to other Persons, aside from outside counsel, until the Court has ruled.

(i) “In-House Counsel” means any lawyer employed by a Party as well as any paralegals, administrative assistants, and clerical and administrative personnel supervised by that lawyer and employed by that Party. In-House Counsel, however, does not include: 1) attorneys employed by the State Plaintiffs; or 2) Outside Counsel.

(j) “Investigation” means the pre-complaint inquiry by the State Plaintiffs into potential anticompetitive conduct by Defendant Google.

(k) “Investigation Materials” means non-privileged documents, testimony or other materials that: (i) any Non-Party provided to any Party, either voluntarily or under compulsory process, relating to the Investigation; (ii) constitute any communication between any Party and any Non-Party in connection with and during the Investigation; (iii) any Party provided to any Non-Party relating to the Investigation; and/or (iv) a Defendant, or affiliated person or entity, provided to a State Plaintiff relating to the Investigation. For the avoidance of doubt, the Investigation Materials are governed by the terms of this Order. To the extent that any Investigation Materials are clawed back for any reason, the procedures set forth at Paragraph 12 of this Order shall apply and, as to State Plaintiffs, such procedures will supersede any other applicable claw back procedures governing the Investigation Materials including those set forth in the Texas OAG Order and the Multistate Confidentiality Agreement.

(l) “Litigation Materials” means non-privileged documents, testimony, or other materials that: (i) any Non-Party provides to any Party, either voluntarily or under compulsory process, in connection with and during the pendency of any of the Actions; (ii) constitute any communication between any Party and any Non-Party in connection with and during the pendency of any of the Actions; (iii) a Defendant provides to any Plaintiff in connection with and during the pendency of any of the Actions; and/or (iv) any Plaintiff provides to any Defendant in connection with and during the pendency of any of the Actions.

(m) “Non-Party” means any natural person, partnership, corporation, association, or other legal entity not named as a Party in any Action.

(n) “Outside Counsel” means the attorneys employed by outside law firms who are retained to represent or advise a Party in any of the Actions, as well as any paralegals, administrative assistants, and clerical and administrative personnel supervised by those lawyers and employed by those Outside Counsel. To the extent any Outside Counsel has not filed an appearance in any of the Actions (“Non-Appearing Law Firm”), a Party shall notify the other Parties of the name of the Non-Appearing Law Firm at least seven days before any attorneys of the Non-Appearing Law Firm obtain access to any Investigation Materials and/or Litigation Materials. Attorneys of the Non-Appearing Law Firm who are given access to Investigation Material and/or Litigation Material, shall first complete and execute an Agreement Concerning Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto.

(o) “Party” means any Plaintiff or Defendant in these Actions. “Parties” collectively means Plaintiffs and Defendants in the Actions.

(p) “Plaintiffs” means the Plaintiffs in each of the Actions, including all of their employees, agents, and representatives.

(q) “Person” means any natural person, corporate entity, business entity, partnership, association, joint venture, governmental entity, or trust.

(r) “Producing Party” shall mean a Party who produced or produces Investigation Material, Litigation Material, or Source Code.

(s) “Protected Person” means any Person (including a Party or a Non-Party) that either voluntarily or under compulsory process, has provided or provides: (i) Investigation Materials, or (ii) Litigation Materials.

(t) “Receiving Party” shall mean a Party who received or receives Investigation Material, Litigation Material, or Source Code.

(u) “Source Code” means extremely sensitive information or items representing computer code and associated comments and revision histories, formulas, engineering specifications, or schematics that define or otherwise describe in detail the algorithms or structure of software or hardware designs, disclosure of which to another Party or Non-Party would create a substantial risk of serious harm that could not be avoided by less restrictive means. To the extent production of Source Code becomes necessary in this case, a Party who produces Source Code may designate it as “Highly Confidential – Source Code.” The protocols for Google’s production of Source Code, and the review of such Source Code, appear in Appendix B to this Order.

(v) “State Plaintiffs” means the States of Texas, Alaska, Arkansas, Idaho, Indiana, Kentucky, Florida, Louisiana, Mississippi, Montana, Missouri, Nevada, North Dakota, South Dakota, South Carolina, Utah, the Commonwealth of Kentucky and Puerto Rico, and any other state that joins an Action.

(w) “State Plaintiffs’ Counsel” shall mean attorneys who work within the Attorney General’s office of a State Plaintiff.

B. Designation of Highly Confidential Information and Confidential Information

2. Within five business days of the Court’s entry of this Order, each Party shall send by email, facsimile, or overnight delivery a copy of this Order to any Non-Party Protected Person (or, if represented by counsel, the Non-Party Protected Person’s counsel) that provided Investigation Materials to that Party.

3. **Designation of Investigation Materials as Confidential or Highly Confidential by Protected Persons.** To the extent a Protected Person has already designated Investigation Materials as Confidential or Highly Confidential, including under the protective order entered in

Texas v. Google, LLC, No. 4:20-cv-957-SDJ (E.D. Tex.), Dkt. 101, those materials shall retain those existing designations, subject to any later challenge by a Party. To the extent that Investigation Materials are reproduced in the Actions, all protections afforded to Litigation Materials pursuant to this Order shall apply.

4. Investigation Materials that have not been designated as Highly Confidential shall be treated as Confidential Information for purposes of this Order pursuant to the Antitrust Civil Process Act, or any other federal or state statute or regulation, or under any federal or state court precedent interpreting such statute or regulation, as well as any information that discloses the substance of the contents of any Confidential Information derived from a document subject to this Order, and any information taken from any portion of such material.

5. The identity of a Non-Party submitting such Highly Confidential Information or Confidential Information shall also be treated as Highly Confidential Information or Confidential Information for the purposes of this Order where the submitter has requested such confidential treatment.

6. Any production of documents or testimony not designated as Confidential or Highly Confidential Information will not be deemed a waiver of any future claim of confidentiality concerning such information if it is subsequently designated as Confidential or Highly Confidential Information. If at any time before trial of these Actions, a Protected Person realizes that it should have designated as Confidential or Highly Confidential Information any Investigation Materials, Litigation Materials, or Source Code that Person previously produced, it may so designate such Documents, testimony, or other materials by notifying the Parties in writing, and, to the extent the new designations relate to Documents, an overlay file with the new designations shall also be provided in accordance with Paragraph 7(g). The Parties shall thereafter

treat the Investigation Materials, Litigation Materials, or Source Code pursuant to the Protected Person's new designation under the terms of this Order. However, the disclosure of any information for which disclosure was proper when made will not be deemed improper regardless of any such subsequent confidentiality designation.

7. **Designation of Litigation Materials as Highly Confidential or Confidential by Protected Persons.** The following procedures govern the process for Protected Persons to designate as Highly Confidential or Confidential any information that they disclose in these Actions, including, but not limited to, information in response to requests under Fed. R. Civ. P. 30, 31, 33, 36, and 45, and Documents disclosed in response to Fed. R. Civ. P. 33(d), 34(b)(2) and (c), or 45:

(a) Indiscriminate designations are prohibited.

(b) **Testimony.** All transcripts of depositions taken in these Actions after entry of this Order will be treated as Highly Confidential Information in their entirety for 45 days after the date of the deposition, or until 5 days before trial, whichever date is earlier. Parties will be responsible for obtaining the deposition transcript for any Party⁴ deponents. For Non-Party deponents, if requested by the Non-Party deponent, the Party who noticed the deposition shall, within 5 business days of being provided a final transcript (subject to any errata) of the deposition (or as soon as reasonably possible after the request is made), provide the final transcript (subject to any errata) to the Non-Party deponent (or the Non-Party deponent's counsel, if applicable). Within 45 days following the date of the deposition, the deponent, whether a Non-Party or a Party, may designate, subject to the provisions of this Order, Highly Confidential Information or Confidential Information any portion of the deposition transcript, by page(s) and line(s), and any

⁴ For purposes of this provision, the term "Party" includes 30(b)(6) witnesses, and a Party's employees and former employees.

deposition exhibits provided by the deponent or the deponent's employer or its affiliates, or containing the Highly Confidential Information or Confidential Information of the deponent or the deponent's employer or its affiliates (regardless of who provided or produced the Document). To be effective, such designations must be provided in writing to the Parties. All transcripts of depositions taken in these Actions after entry of this Order will be treated as Highly Confidential Information in their entirety until the deadline for the deponent to designate portions of the transcript as Highly Confidential Information has expired. Further, to the extent that a Party's Highly Confidential or Confidential Documents were utilized in the deposition, that Producing Party also has 45 days following the date of the deposition to designate any portion of the deposition testimony as Highly Confidential or Confidential to the extent the deposition testimony discloses or relates to Highly Confidential or Confidential Documents used at the deposition. To be effective, such designations must be provided in writing to the Parties' counsel.

When a Party is entitled under this Order to question a deponent about a Document or information that has been designated by a Non-Party as Highly Confidential or Confidential, and such Non-Party is not in attendance at the deposition, the Party that asked such questions shall designate as Highly Confidential or Confidential the portion of the transcript relating to such Highly Confidential or Confidential Document or information.

(c) **Documents.** A Protected Person who designates as Highly Confidential Information any Document that it produced in these Actions must stamp or otherwise mark each Document containing said information with the designation "HIGHLY CONFIDENTIAL" in a manner that will not interfere with legibility, including page numbering, or audibility unless such Document is produced in native electronic format. A Protected Person who designates as Confidential Information any Document that it produced in this Action must stamp or otherwise

mark each Document containing said information with the designation “CONFIDENTIAL” in a manner that will not interfere with legibility, including page numbering, or audibility. Any Document that contains Confidential Information or Highly Confidential Information may be so designated in its entirety. To the extent a Document is produced in native form, such Documents shall be produced in accordance with Paragraph 7(d) below.

(d) **Electronic Documents and Data.** Where a Protected Person produces Confidential or Highly Confidential electronic files and Documents in native electronic format, such electronic files and Documents shall be designated by the Protected Person for protection under this Order by appending to the file names or designators’ information indicating whether the file contains Highly Confidential Information or Confidential Information, or by any other reasonable method for appropriately designating such information produced in electronic format, including by including a slip sheet associated with the electronic file or by making such designations in reasonably accessible metadata associated with the files. Where Highly Confidential Information or Confidential Information is produced in electronic format on a disk or other medium that contains exclusively confidential information, the “HIGHLY CONFIDENTIAL” or “CONFIDENTIAL” designation may be placed on the disk or other medium. When electronic files or Documents in native form are printed for use at a deposition, in a court proceeding, or for provision in printed form to any person who may receive such files in accordance with this Order, the Party printing the electronic files or Documents shall include the slip sheet identifying the electronic file or Document as “HIGHLY CONFIDENTIAL” or “CONFIDENTIAL” along with the production number or Bates number and designation associated with the native file, or shall affix a legend to the printed Document saying “HIGHLY

CONFIDENTIAL” or “CONFIDENTIAL” and include the production number or Bates number and designation associated with the native file.

(e) **Upward Designation of Litigation Materials Produced by Other Parties or Non-Parties.** A Protected Person may upward designate (*i.e.*, change any Litigation Materials produced without a designation to a designation of “Confidential” or “Highly Confidential” or designate any Litigation Materials produced as “Confidential” to a designation of “Highly Confidential”) any Litigation Materials produced by another Protected Person, provided that said Litigation Materials contains the upward designating Protected Person’s own Confidential Information or Highly Confidential Information.

(f) Upward designation shall be accomplished by providing written notice to the Parties and the relevant disclosing Protected Person identifying the Litigation Materials to be re-designated within 120 days from the date of the production containing the materials the Protected Person seeks to upwardly designate, or 30 days prior to trial in an Action, whichever is earlier. Such notice must identify (by Bates number, or in the event there is no Bates number, by other individually identifiable information) each Document the Protected Person wishes to upward designate, and include an explanation as to why the Protected Person wishes to upward designate such Documents, and why the existing confidentiality designation is insufficient. The Protected Person shall also provide an overlay file reflecting the new designations in accordance with Paragraph 7(g). Failure to upward designate within 120 days, alone, will not prevent a Protected Person from obtaining the agreement of the disclosing Protected Person to upward designate certain Litigation Materials or from moving the Court for such relief. Any Party may object to the upward designation of Litigation Materials pursuant to the procedures set forth in Paragraph 13 regarding challenging designations.

(g) **Overlay Files.** To the extent this Order requires a Protected Person to provide an overlay file in connection with a new or altered confidentiality designation, that Protected Person shall have five business days from the date of the changed designation to produce an overlay file. In the interim, the Parties shall take care to treat the Documents at issue as if the new designation applies. For the avoidance of doubt, a Party does not violate this provision where it in good faith attempts to comply with the new designation.

8. In the event that a Party is required by a valid discovery request in any of the Actions to produce Documents designated by a Non-Party or Party as Highly Confidential Information or Confidential Information, then the Party shall:

(a) promptly notify in writing the Party seeking the Highly Confidential Information or Confidential Information that some or all of the information requested is subject to a confidentiality order;

(b) promptly notify the Non-Party or Party that its Highly Confidential Information or Confidential Information is being requested and make the information requested available for inspection by the Non-Party or Party; and

(c) promptly provide the Non-Party or Party with a copy of this Order, the relevant discovery request(s), and a reasonably specific description of the information requested.

9. If the Non-Party or Party fails to object or seek a protective order from this Court within 14 days of receiving the notice and accompanying information, the Non-Party or Party's Highly Confidential Information or Confidential Information responsive to the discovery request may be produced. If the Non-Party or Party timely seeks a protective order, its Highly Confidential Information or Confidential Information shall not be produced before a determination by the

Court.⁵ Absent an order to the contrary, the Non-Party or Party shall bear the burden and expense of seeking protection in this Court of its Highly Confidential Information or Confidential Information. The terms of this Order are applicable to information produced by a Non-Party or Party in the Actions and designated as Highly Confidential Information or Confidential Information. Such information produced by Non-Parties or Parties in connection with these Actions is protected by the remedies and relief provided by this Order. Nothing in these provisions should be construed as prohibiting a Non-Party or Party from seeking additional protections.

10. Unauthorized disclosure of Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code.

(a) In the event of a disclosure of any Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code to any person(s) not authorized to receive such disclosure under this Order, the Party who discovers such unauthorized disclosure shall promptly notify the Protected Person whose material has been disclosed and provide to such Protected Person all known relevant information concerning the nature and circumstances of the disclosure. If it is readily discernible which Party is responsible for the disclosure, the disclosing Party shall also promptly take all reasonable measures to retrieve the improperly disclosed material and to ensure that no further unauthorized disclosure and/or use thereof is made; (b) inform the Person(s) to whom unauthorized disclosure was made of all the terms of this Order; and (c) request such Person(s) execute the Agreement Concerning Confidentiality in the form of Appendix A attached hereto. If it is not readily discernible which Party is responsible for the disclosure, the Parties shall work together to: (a) promptly take all reasonable measures to retrieve the improperly disclosed material and to ensure that no further unauthorized disclosure and/or use thereof is made;

⁵ The purpose of this provision is to alert the interested parties to the existence of confidentiality rights of a Non-Party and to afford the Non-Party an opportunity to protect its confidentiality interests in this Court.

(b) inform the Person(s) to whom unauthorized disclosure was made of all the terms of this Order, and (c) request such Person(s) execute the Agreement Concerning Confidentiality in the form of Appendix A attached hereto.

11. Unauthorized or inadvertent disclosure shall not change the confidential status of any disclosed material or waive the Producing Party's right to maintain the disclosed material as containing Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code.

C. Privileged Investigation Materials and Litigation Materials

12. (a) The production of privileged or work-product protected Documents, electronically stored information ("ESI") or information, whether inadvertent or otherwise, is not a waiver of the privilege or protection from discovery in this case or in any other federal or state proceeding. This Order shall be interpreted to provide the maximum protection allowed by Federal Rule of Evidence 502(d). Federal Rule of Evidence 502(b) shall not apply to any disputes regarding Investigation Material or Litigation Material.

(b) Nothing contained herein is intended to or shall serve to limit a Party's right to conduct a review of Documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production.

(c) If the Producing Party becomes aware that it has produced information protected by the attorney-client privilege or any other privilege or immunity, the Producing Party will promptly notify each Receiving Party in writing of the production and the basis of the privilege being asserted. After being notified, a party must promptly return, sequester,⁶ or destroy the specified information and any copies or summaries it has; must not use or disclose the information

⁶ For the avoidance of doubt, subject to the rights of the Privilege Committee described in this paragraph, sequestration prohibits the Party in possession from further review of the material once a claim of privilege is made.

until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim in camera. However, if the Party has already reviewed the information prior to being notified, four total attorneys⁷ for Plaintiffs (the “Plaintiffs’ Privilege Committee”) or two attorneys for each Defendant (the “Defendants’ Privilege Committees” and, together with the Plaintiffs’ Privilege Committee, the “Privilege Committees”) may review the document for the sole purpose of determining whether to challenge the privilege claim, but they may not quote or attach the information, or disclose the substance of the information, when making the challenge or otherwise use or discuss the information contained therein except in a submission made to the Court in Chambers with a proposed order sealing the submission.⁸ Any such challenge must be made promptly. The Producing Party must preserve the information until the claim is resolved.

(d) If a Receiving Party becomes aware that it is in receipt of information or material that it knows or reasonably should know is privileged, counsel for the Receiving Party shall immediately take steps to: (i) stop reading such information or material; (ii) notify counsel for the Producing Party of such information or material; (iii) collect all copies of such information and material; and (iv) return to the Producing Party and/or destroy such information or material (and, in the case of destruction, certify that fact to the Producing Party if requested to do so). Any

⁷ In addition to the four total attorneys, and any individuals with administrative authority over the document database in which the information resides, shall also be permitted to access the information solely for purposes of processing the clawback and assisting in any challenge of the privilege claim.

⁸ The four-member Plaintiffs’ Privilege Committee shall be composed of one lawyer designated by the State Plaintiffs, the publisher class action, the advertiser class actions, and, collectively, the individual actions. Within 30 days after the entry of this Order, the Parties shall notify each other of the members of the Privilege Committees. The Parties must also provide notice of any changes to the Privilege Committees along with the reason for such change.

notes or summaries referring or relating to such material shall be destroyed simultaneously therewith.

(e) This Order is without prejudice to any Protected Person's right to assert that any Investigation Materials or Litigation Materials are subject to any applicable claim of privilege or protection, including, but not limited to, the attorney-client privilege and the work-product doctrine, and it is without prejudice to any Party's right to contest such a claim of privilege or protection.

D. Objections to Confidentiality Designations

13. Any Party who objects to any confidentiality designation, or part thereof, (the "Objecting Party") may, until 30 days before the trial of its Action, provide a written notice to the Protected Person who made such designation (the "Designating Party") and to all Parties stating with particularity the grounds for the objection. All materials objected to shall continue to be treated as Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code pending resolution of the dispute. Within 10 days of the Objecting Party's written notice, the Objecting Party and the Designating Party shall attempt to confer to discuss their respective positions. If the Objecting Party and Designating Party cannot reach an agreement on the objection within 10 days of the Objecting Party's written notice (or another deadline agreed to by the Objecting Party and the Designating Party), the Objecting Party may raise the dispute to this Court by filing a letter motion and/or motion in accordance with the applicable rules and/or the Court's Individual Practices. If the Court finds the designation of Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code to have been inappropriate, the challenged designation shall be considered rescinded, and the Designating Party shall reproduce the Documents with the revised designations, along with an overlay file in

accordance with Paragraph 7(g). Notwithstanding anything else contained in this Order, the Parties reserve their rights under Fed. R. Civ. P. 37.

E. Disclosure of Highly Confidential Information or Confidential Information

14. Highly Confidential Information may be disclosed only to the following Persons:

- (a) the Court and all Persons assisting the Court in the Actions, including law clerks, court reporters, and stenographic or clerical personnel;
- (b) Outside Counsel for a Party, including any attorneys, paralegals, and other professional personnel (including support and IT staff) that such outside counsel assigns to the Actions whose functions require access to the information (but not any employee of a Party);
- (c) State Plaintiffs' Counsel and paralegals, and other professional personnel (including support and IT staff) that such State Plaintiff's Counsel assign to the Actions whose functions require access to the information;
- (d) Designated In-House Counsel of a Party, if, prior to July 19, 2023, such counsel was properly designated pursuant to the procedures set forth in Paragraph 20 of the Confidentiality Order, Dkt. 297, entered May 1, 2022.
- (e) outside vendors or service providers (such as copy-service providers, outside court reporters retained for depositions, document-management consultants, or lawyers or law firms for document review other than Outside Counsel) and agents or independent contractors retained by a Party to assist that Party in an Action provided that they shall first execute an Agreement Concerning Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto;
- (f) any mediator, arbitrator, or special master that the Parties engage in this Action or that this Court appoints provided that they shall first execute an Agreement Concerning

Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto;

(g) any Person who the Highly Confidential Information itself indicates, or who the Receiving Party has a good-faith basis to believe, was the author, addressee, recipient, custodian, or source of the Document or Highly Confidential Information.

(h) any Person who the Highly Confidential Information itself indicates, or who the Receiving Party has a good-faith basis to believe, had lawful access to the Document or the Highly Confidential Information;

(i) during a deposition, any Person who the Highly Confidential Information itself indicates, or who the Receiving Party has a good-faith basis to believe, had knowledge of the Highly Confidential Information;

(j) during a deposition, any current employee of the Designating Party;

(k) any Person retained by a Party to serve as a testifying or consulting expert in these Actions,⁹ including any employees of the firm with which the expert or consultant is associated and independent contractors who assist the expert's work in the Actions, provided that they shall first execute an Agreement Concerning Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto;

(l) outside trial consultants (including, but not limited to, graphics consultants), provided that they shall first execute an Agreement Concerning Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto;

⁹ This provision does not apply to any Person retained by a Party to serve as a testifying or consulting expert, where such person is also an employee of a Party.

(m) Any Person as may be authorized by written agreement of the Designating Party, verbal agreement of the Designating Party on the record at a deposition or Court hearing, or by order of the Court.

15. Confidential Information may be disclosed only to the following Persons:

(a) the Court and all Persons assisting the Court in the Actions, including law clerks, court reporters, and stenographic or clerical personnel;

(b) Outside Counsel for a Party, including any attorneys, paralegals, and other professional personnel (including support and IT staff) that such outside counsel assigns to the Actions whose functions require access to the information (but not any employee of the Party)

(c) State Plaintiffs' Counsel and paralegals, and other professional personnel (including support and IT staff) that such State Plaintiff's Counsel assign to the Actions whose functions require access to the information;

(d) the officers, directors, and employees (including In-House Counsel) of a Party to whom disclosure is reasonably necessary for this litigation and who have signed the Agreement Concerning Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto;

(e) outside vendors or service providers (such as copy-service providers, outside court reporters retained for depositions, document-management consultants, or lawyers or law firms for document review other than Outside Counsel) and agents or independent contractors retained by a Party to assist that Party in the Actions provided that they shall first execute an Agreement Concerning Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto;

(f) any mediator, arbitrator, or special master that the Parties engage in the Actions or that this Court appoints provided that they shall first execute an Agreement Concerning Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto;

(g) any Persons who the Confidential Information itself indicates, or who the Receiving Party has a good-faith basis to believe, was the author, addressee, recipient, custodian, or source of the Document or Confidential Information;

(h) any Persons who the Confidential Information itself indicates, or who the Receiving Party has a good faith basis to believe had lawful access to the Document or Confidential Information;

(i) during a deposition, any Persons who the Confidential Information itself indicates, or who the Receiving Party has a good-faith basis to believe, had knowledge of the Confidential Information;

(j) any Person whose statements or communications are quoted, recounted, or summarized in said Party's Documents or Confidential Information, except that only those portions of the Documents or Confidential Information quoting, recounting, or summarizing a Person's statements or communications may be disclosed to that Person;

(k) during a deposition, any current employee of the Designating Party

(l) outside trial consultants (including, but not limited to, graphics consultants) provided that they shall first execute an Agreement Concerning Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto;

(m) any Person retained by a Party to serve as a testifying or consulting expert in these Actions,¹⁰ including any employees of the firm with which the expert or consultant is associated and independent contractors who assist the expert's work in the Actions, provided that they shall first execute an Agreement Concerning Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto;

(n) any Person as may be authorized by written agreement of the Designating Party, verbal agreement of the Designating Party on the record at a deposition or Court hearing, or by order of the Court.

16. The Parties shall have the right to seek redress from this Court to enforce the provisions of the Agreement Concerning Confidentiality set forth in Appendix A with respect to any Person bound by this Confidentiality Order.

17. Each Person described in Paragraphs 14 and 15 of this Order to whom information designated as Highly Confidential Information or Confidential Information is disclosed must not disclose that Highly Confidential Information or Confidential Information to any other Person, except as permitted in this Order.

18. Nothing in this Order:

(a) limits a Protected Person's use or disclosure of its own information designated as Highly Confidential Information or Confidential Information;

(b) prevents disclosure of Highly Confidential Information or Confidential Information with the consent of the Protected Person that designated the material as Confidential or Highly Confidential;

¹⁰ This provision does not apply to any Person retained by a Party to serve as a testifying or consulting expert, where such Person is also an employee of a Party.

(c) prevents disclosure by a Party of Highly Confidential Information or Confidential Information: (i) that is or has become publicly known through no fault of that Party; (ii) lawfully acquired by or known to that Party independent of receipt during the Investigation or in discovery in the Actions; (iii) previously produced, disclosed and/or provided to that Party without an obligation of confidentiality and not by inadvertence or mistake; or (iv) pursuant to an order of a court or as may be required by regulation;

(d) prevents counsel from rendering advice to his or her client with respect to this matter or from generally referring to or relying upon Confidential Information or Highly Confidential Information in rendering such advice so long as counsel does not specifically disclose the substance of the Confidential Information or Highly Confidential Information; or

(e) prevents State Plaintiffs' retention, use, or disclosure of Investigation Materials outside the context of the Actions to the extent permitted by applicable law or regulation governing such pre-complaint discovery, or for law enforcement purposes, or as required by law, court order, or regulation. Any such disclosures shall be limited to those permitted by applicable law or regulation. State Plaintiffs will not disclose any Litigation Materials produced only during the pendency of the Actions to any Non-Party, except as ordered by a court or as may be required by regulation and subject to Paragraph 27. If Investigation Materials or Litigation Materials are requested for disclosure under a state's public information act or the equivalent, this Order prohibits disclosure to the extent the state's public information act or the equivalent provides an exception for disclosure of information protected by court order.

F. Disclosure of Highly Confidential Information to Designated In-House Counsel for Parties Based on Need

19. A Party may at any time before the trial of its Action request disclosure of Highly Confidential Information to Designated In-House Counsel, not covered under Paragraph 14(d), by

consent of the Designating Party or motion with the Court. Unless otherwise ordered by the Court or agreed to in writing by the Designating Party, a Party seeking to disclose Highly Confidential Information to Designated In-House Counsel must submit in writing to the other Parties and the Designating Person a written statement that: (1) describes with particularity the Highly Confidential Information the Party seeks to disclose to Designated In-House Counsel; (2) sets forth the full name of each Designated In-House Counsel and the city and state of his or her residence, and (3) describes each Designated In-House Counsel's primary job duties and responsibilities in sufficient detail to determine if each Designated In-House Counsel is involved in Competitive Decision-Making. The Party must meet and confer with the Designating Party to try to resolve the matter by agreement within seven days of the written notice. If no agreement is reached, the Party may file a motion with the Court. The other Parties and/or the Designating Party will have seven days to respond to such motion. The Party will not disclose any Highly Confidential Information to the Designated In-House Counsel pending resolution of the dispute. If the Court finds that the Designated In-House Counsel has a particularized need for access to the Highly Confidential Information that outweighs the risk of harm to the Designating Party or the public interest, the Party will be permitted to disclose the Highly Confidential Information to the Designated In-House Counsel.

G. Use of Information Designated Highly Confidential or Confidential in this Action

20. In the event that any Highly Confidential Information or Confidential Information is contained in any pleading, motion, exhibit, or other paper filed or to be filed with the Court, the Court shall be so informed by the Party filing such papers, and such papers shall be filed under seal, in accordance with the Court's Individual Practice 5(B), as modified by the terms of this Order. The Parties agree to act in good faith to limit the need to seal Documents filed in this Court.

21. **Filing Highly Confidential Information or Confidential Information Under Seal.** Notwithstanding any other provision, no document may be filed with the Clerk under seal without a further Order of this Court addressing the specific documents or portions of documents to be sealed. Any application to seal shall be accompanied by an affidavit or affidavits and a memorandum of law, demonstrating that the standards for sealing have been met and specifically addressing the applicability of *Lugosch v. Pyramid Co. of Onondaga*, 435 F.3d 110, 119-120 (2d Cir. 2006) and any other controlling authority. Unless otherwise ordered, a Party seeking to file another Party or Non-Party's Highly Confidential Information or Confidential Information shall so advise the other Party or Non-Party seven business days in advance specifying the precise portion of the information the Party seeks to use, the general purpose thereof and any redactions to which the Party does not object. Within five business days thereafter, the Party or Non-Party whose Highly Confidential Information or Confidential Information is sought to be used may make an application to seal, indicating the portion or portions of the information it seeks to have sealed. If a Party's deadline or need to file a pleading that contains Highly Confidential or Confidential Information is short such that complying with this paragraph's requirements would be unduly burdensome, the Parties agree to discuss in good faith a reasonable extension of these deadlines subject to the Court's approval. Nothing herein is intended to alter or modify the applicability of Rule 5.2, Fed. R. Civ. P., to this case. The redactions expressly authorized by Rule 5.2 may be made without further application to the Court.

22. Parties shall give the other Parties notice (a minimum of two business days) if they reasonably expect a deposition, hearing, or other proceeding to include Highly Confidential Information so that the other parties can ensure that only authorized individuals are present during the portions of those proceedings where the Highly Confidential Information may be used. The

use of a Document as an exhibit at a deposition shall not in any way affect its designation as Highly Confidential Information or Confidential Information.

H. Use of Highly Confidential Information or Confidential Information at Trial

23. Disclosure at trial or at any evidentiary hearing of any Document, testimony, or other material designated as Highly Confidential Information or Confidential Information will be governed pursuant to a separate court order. Unless otherwise directed by the Court, the Parties shall meet and confer and submit a recommended order outlining those procedures no later than 30 calendar days before the first day of trial or any evidentiary hearing. Upon the filing of a proposed order governing the disclosure of Highly Confidential Information or Confidential Information at trial or any evidentiary hearing, the Parties shall provide notice of such order to Non-Parties whose Highly Confidential Information or Confidential Information is expected to be used at trial or any evidentiary hearing.

24. Unless otherwise provided for in this Order, all Highly Confidential Information and Confidential Information produced by a Party or a Non-Party in any of the Actions shall be used solely for the conduct of these Actions and shall not be used by a Party, Non-Party, or any Person subject to this Order, including counsel for a Party or Non-Party, for any business, commercial, competitive, personal, or other purpose. Such Highly Confidential and Confidential Information may only be disclosed under the conditions described in this Order.

I. Investigation Materials or Litigation Materials Subpoenaed or Ordered Produced in Other Litigation

25. If a Party is served with a lawful subpoena or a court order issued by a court, arbitral, administrative, or legislative body, or with a court order issued in other litigation that compels disclosure of any information or items designated in any of the Actions as Confidential or Highly Confidential that Party must:

(a) promptly notify in writing the Designating Party (such notification shall include a copy of the subpoena or court order);

(b) promptly notify in writing the Person or entity who issued the subpoena or caused the order to issue in the other litigation, that some or all of the material covered by the subpoena or order is subject to this Order (such notification shall include a copy of this Order); and

(c) cooperate with respect to all reasonable procedures sought to be pursued by the Designating Party whose Highly Confidential or Confidential Information may be affected.¹¹

26. If the Designating Party timely¹² seeks a protective order, the Party served with the subpoena or court order shall not produce any information designated in these Actions as Confidential or Highly Confidential before a determination by the court from which the subpoena or order issued, unless the Party has obtained the Designating Party's permission. The Designating Party shall bear the burden and expense of seeking protection in that court of its Confidential Information or Highly Confidential Information – and nothing in these provisions should be construed as authorizing or encouraging a Receiving Party in these Actions to disobey a lawful directive from another court.

27. If, under any public records or other relevant law, any Investigation Materials or Litigation Materials are subject to any form of compulsory process in a Plaintiff State or is demanded from a Plaintiff State, such Plaintiff State shall notify in writing the Designating Party

¹¹ The purpose of imposing these duties is to alert the interested parties to the existence of this Order and to afford the Designating Party in this case an opportunity to try to protect its confidentiality interests in the court or other tribunal from which the subpoena or order issued.

¹² The Designating Party shall have at least 14 days from the service of the notification pursuant to Paragraph 25(a) to seek a protective order, unless the subpoena or order requires a response within a period shorter than 14 days, or unless a shorter period applies under the rules of the court or other tribunal from which the subpoena or order issued, in which case such rules shall apply.

whose Investigation Materials or Litigation Materials may be affected within 10 business days of receiving the process or demand and before producing Investigation Materials or Litigation Materials, unless state statute, or court order or other public adjudicatory body requires that the Plaintiff State produce the Investigation Materials or Litigation Materials in a shorter time frame. The State shall not produce the Investigation Materials or Litigation Materials in response to such compulsory process or public records request unless the Plaintiff State deems that it is required by law to do so and provides 10 business days' notice of its intent to do so to the Designating Party, unless state statute, or court order or other public adjudicatory body requires that the Plaintiff State produce the Investigation Materials or Litigation Materials in a shorter time frame. However, if a Plaintiff State denies a public records or similar request and the denial is not challenged, the Plaintiff State does not need to provide notice pursuant to this paragraph. If Investigation Materials or Litigation Materials are requested for disclosure under a state's public information act or the equivalent, this Order prohibits disclosure to the extent the state's public information act or the equivalent provides an exception for disclosure of information protected by court order. Nothing contained herein shall alter or limit the obligations of a Plaintiff State that may be imposed by statute or court order regarding the disclosure of Documents and information supplied to the state.

J. Procedures upon Termination of this Action

28. The obligations imposed by this Order survive the termination of the Actions unless the Court, which shall retain jurisdiction to resolve any disputes arising out of this Order, orders otherwise. Within 90 days after the expiration of the time for appeal of an order, judgment, or decree terminating an Action, all Persons, other than State Plaintiffs, in such Action having received information designated as Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code must return all copies thereof to the Protected Person (or the Protected Person's counsel if represented by counsel) that produced it or destroy or delete all

copies of such Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code and certify that fact in writing to the Party or Protected Person. Within 90 days after the expiration of the time for appeal of an order, judgment, or decree terminating an Action, all State Plaintiffs in such Action having received information designated as Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code must, to the extent permitted by State Plaintiffs' retention schedules, either make a good-faith effort to return all copies thereof to the Protected Person (or the Protected Person's counsel if represented by counsel) that produced it or destroy or delete all copies of such Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code.

29. Counsel for the Parties will be entitled to retain court papers and exhibits, deposition transcripts and exhibits, hearing transcripts and exhibits, trial transcripts and exhibits, correspondence (including internal correspondence and email) and work product, provided that the Parties and their counsel do not disclose the portions of these materials containing information designated as Highly Confidential Information or Confidential Information to any Person, except pursuant to court order or agreement with the Protected Person that produced the Highly Confidential Information or Confidential Information or as otherwise permitted herein. All Highly Confidential Information and Confidential Information returned to the Parties or their counsel by the Court likewise must be disposed of in accordance with this paragraph. Nothing in this paragraph, however, restricts the rights of the Parties under Paragraphs 14 and 15 of this Order.

K. New Parties to The Actions

30. In the event that additional Persons or entities become parties to an Action, such new Parties shall not have access to Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code produced by or obtained from any Protected Person until an authorized person executes, on behalf of the new Party, an Agreement Concerning

Confidentiality agreeing to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto.

L. Non-Parties

31. Any Party, in conducting discovery from Non-Parties in connection with the Actions, shall provide any Non-Party from which it seeks discovery with a copy of this Order so as to inform each such Non-Party of his, her or its rights herein. If a Non-Party provides discovery to any Party in connection with the Actions, the provisions of this Order shall apply to such discovery as if such discovery were being provided by a Party. Under such circumstances, if the Non-Party agrees to be bound by the terms of this Confidentiality Order in the form of Appendix A attached hereto, the Non-Party shall have the same rights and obligations under the Order as held by the Parties, except that, other than with leave of court, in no circumstance may a Party's Highly Confidential Information be disclosed to a Non-Party without the consent of that Party. However, a Party's Highly Confidential Information may be shared with a former employee of that Party if the former employee may view the Highly Confidential Information pursuant to Paragraph 14.

M. Reservation of Rights

32. Nothing contained in this Order or any designation of confidentiality hereunder, or any failure to make such designation, shall be used or characterized by any Party as an admission by a Party or a Party opponent. Nothing in this Order shall be deemed an admission that any particular information designated as Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code is entitled to protection under the Order, Federal Rule of Civil Procedure 26(c), or any other law. Nothing in this Order shall be construed as granting any Person a right to receive specific Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code where a court has entered an order precluding that Person

from obtaining access to that information. The Parties specifically reserve the right to challenge the designation of any particular information as Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code and agree that no Party waives any right it otherwise would have to object to disclosing or producing any information or item on any ground not addressed in this Order. Similarly, no Party waives any right to object on any ground to introduction or use as evidence of any of the Investigation Materials or Litigation Materials covered by this Order.

N. Standard of Care

33. The recipient of any Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code shall maintain such material in a secure and safe area and shall exercise a standard of due and proper care with respect to the storage, custody, use, and/or dissemination sufficient to safeguard against unauthorized or inadvertent disclosure of such material. Confidential Information, Highly Confidential Information, or Highly Confidential — Source Code shall not be copied, reproduced, extracted or abstracted, except for the purpose of the conduct of an Action. All such copies, reproductions, extractions, and abstractions shall be subject to the terms of this Order and be clearly marked to reflect their designation.

O. Right to Seek Modification

34. Nothing in this Order limits any Person, including members of the public, a Party, or a Protected Person, from seeking: (1) further or additional protections of any of its materials, or (2) modification of this Order upon motion duly made pursuant to the Rules of this Court, including, without limitation, an order that certain material not be produced at all or is not admissible evidence in any Action or any other proceeding.

P. The Privacy Act

35. Any order of this Court requiring the production of any Document, information, or transcript of testimony constitutes a court order within the meaning of the Privacy Act, 5 U.S.C. § 552a(b)(11).

Q. Persons Bound by This Order

36. This Order shall be binding on the Parties to the Actions, their attorneys, and their successors, personal representatives, administrators, assigns, parents, subsidiaries, divisions, affiliates, employees, agents, retained consultants and experts, and any persons or organizations over which they have direct control, and any Non-Party, to the extent such Non-Party has agreed to be bound by this Order.

37. All persons subject to this Order are reminded that this Order may be enforced by the Court's full powers of criminal and civil contempt.

SO ORDERED.

Dated: New York, New York
_____, 2023

P. Kevin Castel
United States District Judge

APPENDIX A

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

| | |
|---------------------------------------------------|-----------------------------------|
| In re Google Digital Advertising Antitrust Litig. | Civil Action No. 21-MD-3010 (PKC) |
|---------------------------------------------------|-----------------------------------|

AGREEMENT CONCERNING CONFIDENTIALITY

I, _____, am employed by _____
as _____.

I hereby certify that:

1. I have read the Confidentiality Order (“Confidentiality Order”) entered in the above-captioned action (this “Action”) and understand its terms.

2. I agree to be bound by the terms of the Confidentiality Order entered in this Action. I agree to use the information provided to me only as permitted in this Confidentiality Order.

3. I understand that my failure to abide by the terms of the Confidentiality Order entered in this Action may subject me to civil and criminal penalties for contempt of court.

4. I submit to the jurisdiction of this Court, and specifically the United States District Court for the Southern District of New York, solely for the purpose of enforcing the terms of the

Confidentiality Order entered in the above-captioned action and freely and knowingly waive any right I may otherwise have to object to the jurisdiction of said court.

Signature

Date

APPENDIX B

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

| | |
|----------------------------------------------------------|-----------------------------------|
| <i>In re Google Digital Advertising Antitrust Litig.</i> | Civil Action No. 21-MD-3010 (PKC) |
|----------------------------------------------------------|-----------------------------------|

[PROPOSED] CONFIDENTIALITY ORDER: SOURCE CODE PROTOCOL

A. Restrictions on those who may view Source Code.

1. Unless otherwise ordered by the Court or permitted in writing by the Designating Party, a Receiving Party may disclose any information or item designated Highly Confidential - Source Code only to:

a) the Receiving Party's Outside Counsel of Record in this action, as well as employees of said Outside Counsel of Record to whom it is reasonably necessary to disclose the information for this litigation and who have signed the "Agreement Concerning Confidentiality" that is attached to the Protective Order as Appendix A;

b) up to three Experts (for the avoidance of doubt, the Parties can agree to allow such disclosure to more than three Experts of the Receiving Party) of the Receiving Party (1) to whom disclosure is reasonably necessary for this litigation, (2) who have signed the "Agreement Concerning Confidentiality" (Appendix A), and (3) as to whom the procedures set forth in Paragraph 2 below and specifically identified as eligible to access Highly Confidential – Source Code Information or Items, have been followed;

c) the Court and its personnel;

d) stenographic reporters, videographers and their respective staff who have signed the “Agreement Concerning Confidentiality” (Appendix A) and are transcribing or videotaping a deposition wherein Highly Confidential – Source Code Information or Items are being discussed, provided that such reporters and videographers shall not retain or be given copies of any portions of the source code, which if used during a deposition, will not be attached as an exhibit to the transcript but instead shall be identified only by its production numbers.

e) while testifying at deposition or trial in this action only: (i) any current officer, director, or employee of the Producing Party or original source of the information; (ii) any person designated by the Producing Party to provide testimony pursuant to Rule 30(b)(6) of the Federal Rules of Civil Procedure; and/or (iii) any person who authored, previously received (other than in connection with this litigation), or was directly involved in creating, modifying, or editing the Highly Confidential - Source Code Information or Items, as evident from its face or reasonably certain in view of other testimony or evidence. Persons authorized to view Highly Confidential - Source Code Information or Items pursuant to this sub-paragraph shall not retain or be given copies of the Highly Confidential - Source Code Information or Items except while so testifying.

B. Process for Requesting to Disclose Source Code

2. Unless otherwise ordered by the court or agreed to in writing by the Designating Party, a Party that seeks to disclose to an Expert (as defined in this Order) any information or item that has been designated Highly Confidential - Source Code pursuant to paragraphs 1(b) first must make a written request to the Designating Party that (1) identifies the general categories of Highly Confidential - Source Code information that the Receiving Party seeks permission to disclose to the Expert, (2) sets forth the full name of the Expert and the city and

state of his or her primary residence, (3) attaches a copy of the Expert's current resume, (4) identifies the Expert's current employer(s), (5) identifies each person or entity from whom the Expert has received compensation or funding for work in his or her areas of expertise or to whom the expert has provided professional services, including in connection with a litigation, at any time during the preceding five years, and (6) identifies (by name and number of the case, filing date, and location of court) any litigation in connection with which the Expert has offered expert testimony, including through a declaration, report, or testimony at a deposition or trial, during the preceding five years.

3. A Party that makes a request and provides the information specified in the preceding respective paragraphs may disclose the subject Highly Confidential - Source Code to the identified Expert unless, within 14 days of delivering the request, the Party receives a written objection from the Designating Party. Any such objection must set forth in detail the grounds on which it is based.

4. A Party that receives a timely written objection must meet and confer with the Designating Party (through direct voice to voice dialogue) to try to resolve the matter by agreement within seven days of the written objection. If no agreement is reached, the Party seeking to make the disclosure to the Expert may file a motion in accordance with Local Rules and Individual Practices seeking permission from the court to do so. Any such motion must describe the circumstances with specificity, set forth in detail the reasons why the disclosure to the Expert is reasonably necessary, assess the risk of harm that the disclosure would entail, and suggest any additional means that could be used to reduce that risk. In addition, any such motion must be accompanied by a competent declaration describing the parties' efforts to resolve the matter by agreement (i.e., the extent and the content of the meet and confer discussions) and

setting forth the reasons advanced by the Designating Party for its refusal to approve the disclosure.

5. In any such proceeding, the Party opposing disclosure to the Expert shall bear the burden of proving that the risk of harm that the disclosure would entail (under the safeguards proposed) outweighs the Receiving Party's need to disclose the Protected Material to its Expert.

C. Restrictions on those who may see Source Code (Patent and Acquisition Bars)

6. Absent written consent from the Producing Party, any individual who receives access to information designated Highly Confidential - Source Code by the Producing Party shall not be involved in the prosecution of patents or patent applications relating to the subject matter of this action, including without limitation the patents related to the subject matter of this action and any patent or application claiming priority to the patents related to the subject matter of this action, before any foreign or domestic agency, including the United States Patent and Trademark Office ("the Patent Office"). For purposes of this paragraph, "prosecution" means directly or indirectly drafting, amending, or advising others as to the drafting or amending of patent claims. To avoid any doubt, "prosecution" as used in this paragraph does not include representing a party challenging or defending a patent before a domestic or foreign agency (including, but not limited to, a reissue protest, *ex parte* reexamination, *inter partes* reexamination, *inter partes* review, post grant review or covered business method review). This Prosecution Bar shall begin when access to Source Code information is first received by the affected individual and shall end two (2) years after final termination of this action.

7. Absent written consent from the Producing Party, any individual who receives access to information designated Highly Confidential – Source Code by the Producing Party shall not (i) participate in the acquisition of patents or patent applications relating to the subject

matter of this action for the purposes of assertion against Google LLC; or (ii) advise or counsel clients regarding the same. This Acquisition Bar shall not prohibit counsel from advising clients on other legal matters involving patents, including validity and settlement negotiations. This Acquisition Bar shall begin when access to Source Code information is first received by the affected individual and shall end two (2) years after final termination of this action.

D. Process for Reviewing Source Code

8. To the extent production of source code becomes necessary in this case, a Producing Party may designate material as Highly Confidential – Source Code if it comprises, includes, or substantially discloses confidential, proprietary or trade secret source code or algorithms. This material may include, among things, technical design documentation that comprises, includes, or substantially discloses source code or algorithms.

9. Protected Material designated as Highly Confidential – Source Code shall be subject to all of the protections herein including the Prosecution Bar set forth in Paragraph 6 and the Acquisition Bar set forth in Paragraph 7, and may be disclosed only as set forth in Paragraph 1.

10. Any source code produced in discovery shall only be made available for inspection, not produced except as set forth below, in a format allowing it to be reasonably reviewed and searched, during normal business hours or at other mutually agreeable times, at (1) an office of the Producing Party or the Producing Party's primary outside counsel of record or (2) another mutually agreed upon location. The source code shall be made available for inspection on a secured computer (the "Source Code Computer") in a secured, locked room without Internet access or network access to other computers, and the Receiving Party shall not copy, remove, or otherwise transfer any portion of the source code onto any recordable media or

recordable device. The Producing Party will make a good faith effort to provide legitimate review tools to the Source Code Computer as requested by the Receiving Party. The Receiving Party shall provide a license to the requested review tools should the Producing Party not already have one. The secured computer shall have disk encryption and be password protected. Use or possession of any input/output device (e.g., USB memory stick, mobile phone or tablet, camera or any camera-enabled device, CD, floppy disk, portable hard drive, laptop, or any device that can access the Internet or any other network or external system, etc.) is prohibited while accessing the computer containing the source code. All persons entering the locked room containing the source code must agree to submit to reasonable security measures to ensure they are not carrying any prohibited items before they will be given access to the locked room. The computer containing source code will be made available for inspection during regular business hours (9:00 A.M. to 5:00 P.M. local time), upon reasonable notice to the producing party, which shall not be less than 3 business days in advance of the requested inspection. The Producing Party may visually monitor the activities of the Receiving Party's representatives during any source code review, but only to ensure that there is no unauthorized recording, copying, or transmission of the source code.

11. The Receiving Party may request paper copies of limited portions of source code, but only if and to the extent reasonably necessary for the preparation of court filings, pleadings, expert reports, or other papers, or for deposition or trial and except to the extent allowed in Paragraph 16. The Receiving Party shall not request paper copies for the purposes of reviewing the source code other than electronically as set forth in Paragraph 10 in the first instance. The Producing Party shall undertake to produce the requested material as soon as possible after it is requested, but in no event more than 5 business days after the request, and the Producing Party

will provide the requested material on watermark or colored paper (which shall not prevent the creation of legible copies made only as authorized herein) bearing Bates numbers and the legend Highly Confidential – Source Code unless objected to as discussed below. At the inspecting Party’s request or the request of an Expert retained by the inspecting Party to whom disclosure of material designated Highly Confidential – Source Code is permitted, additional sets (or subsets) of printed source code may be requested and provided by the Producing Party within 5 business days of the request. The Producing Party may challenge the amount of source code requested in hard copy form pursuant to the dispute resolution procedure and timeframes set forth in Paragraph 13 of the Protective Order, whereby the Producing Party is the “Challenging Party” and the Receiving Party is the “Designating Party” for purposes of dispute resolution. Contested printouts do not need to be produced to the Receiving Party until the matter is resolved by the Court.

12. The Receiving Party shall maintain a record of any individual who has inspected any portion of the source code in electronic or paper form. The Receiving Party shall maintain all printed portions of the source code in a secured, locked area under the direct control of counsel (or outside experts or consultants who have been approved to access source code) responsible for maintaining the security and confidentiality of the designated materials. Any paper copies designated Highly Confidential – Source Code shall be stored or viewed only at (i) the offices or working locations of outside counsel for the Receiving Party, (ii) the offices or working locations of outside experts or consultants who have been approved to access source code; (iii) the site where any deposition is taken (iv) the Court; or (v) any intermediate location necessary to transport the information to a hearing, trial or deposition. Except as provided in Paragraph 16 of this Appendix, the Receiving Party shall not create any electronic or other images of the paper

copies and shall not convert any of the information contained in the paper copies into any electronic format. Any printed pages of source code, and any other documents or things reflecting source code that have been designated by the producing party as Highly Confidential – Source Code may not be copied, digitally imaged or otherwise duplicated, except the Receiving Party may make additional paper copies if such additional copies are necessary to prepare court filings, pleadings, or other papers (including a testifying expert's expert report) or necessary for deposition, or as provided below in Paragraph 16. Any paper copies used during a deposition shall be retrieved by the Receiving Party at the end of each day and must not be given to or left with a court reporter or any other unauthorized individual.

13. The Receiving Party's outside counsel and/or expert shall be entitled to take notes relating to the source code but may not copy any portion of the source code into the notes. No copies of all or any portion of the source code may leave the room in which the source code is inspected except as otherwise provided herein. Further, no other written or electronic record of the source code is permitted except as otherwise provided herein.

14. A list of names of persons who will view the source code will be provided to the producing party in conjunction with any written (including email) notice requesting inspection. The Producing Party shall maintain a daily log of the names of persons who enter the locked room to view the source code and when they enter and depart. The Receiving Party shall be entitled to a copy of the log.

15. The Receiving Party's outside counsel shall maintain a log of all copies of the source code in its possession or in the possession of its retained consultants. The log shall include the names of the recipients and reviewers of copies and locations where the copies are stored. Upon request by the Producing Party, the Receiving Party shall provide reasonable

assurances and/or descriptions of the security measures employed by the Receiving Party and/or person that receives a copy of any portion of the source code. The Producing Party shall be entitled to a copy of the log.

16. Except as provided in this paragraph, the Receiving Party may not create electronic images, or any other images, of the source code from the paper copy for use on a computer (e.g., may not scan the source code to a PDF, or photograph the code). The Receiving Party may create an electronic copy or image of limited excerpts of source code only to the extent necessary in a pleading, exhibit, expert report, discovery document, deposition transcript, other Court document, or any drafts of these documents (“Source Code Documents”). The Receiving Party shall only include such excerpts as are reasonably necessary for the purposes for which such part of the Source Code is used. Images or copies of Source Code shall not be included in correspondence between the parties (references to production numbers shall be used instead) and shall be omitted from pleadings and other papers except to the extent permitted herein. The Receiving Party may create an electronic image of a selected portion of the Source Code only when the electronic file containing such image has been encrypted using commercially reasonable encryption software including password protection. The communication and/or disclosure of electronic files containing any portion of source code shall at all times be limited to individuals who are authorized to see source code under the provisions of this Protective Order. Additionally, all electronic copies must be labeled Highly Confidential – Source Code.

17. To the extent portions of source code are quoted in a Source Code Document, either (1) the entire document will be stamped and treated as Highly Confidential – Source Code

or (2) those pages containing quoted Source Code will be separately bound, and stamped and treated as Highly Confidential – Source Code.

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

| | | |
|---------------------------------------------------|--|-----------------------------------|
| In re Google Digital Advertising Antitrust Litig. | | Civil Action No. 21-MD-3010 (PKC) |
|---------------------------------------------------|--|-----------------------------------|

ORDER REGARDING DISCOVERY PROCEDURE

WHEREAS, Rule 26(f) of the Federal Rules of Civil Procedure states that the parties must develop a proposed discovery plan that states the parties' views and proposals on, among other things, "any issues about disclosure, discovery, or preservation of electronically stored information, including the form or forms in which it should be produced," Fed. R. Civ. P. 26(f)(3)(C);

WHEREAS, the parties mutually seek to reduce the time, expense, and other burdens of discovery of certain electronically stored information ("ESI") and privileged materials, as described further below, and to better define the scope of their obligations with respect to preserving such information and materials;

WHEREAS, the parties are aware of the importance of cooperation and commit to cooperate in good faith throughout the matter to promote the "just, speedy, and inexpensive determination" of this action, as required by Fed. R. Civ. P. 1. The parties agree to use reasonable, good faith, and proportional efforts to preserve, identify and produce relevant and discoverable information consistent with Fed. R. Civ. P. 26(b)(1). The parties' cooperation includes identifying appropriate limits to eDiscovery, including limits on custodians, identifying relevant and discoverable subject matter, establishing time periods for eDiscovery and other parameters to limit and guide preservation and eDiscovery issues;

WHEREAS, the parties have not agreed on all aspects of a proposed discovery plan and in ruling on the parties' conflicting proposals the Court has considered the written submissions of the parties and the argument of counsel at the hearing conducted on February 22, 2023, as well as their post-hearing submissions of March 8, 2023;

NOW THEREFORE, it is hereby ORDERED:

I. GENERAL PROVISIONS

1. Except as specifically set forth herein, this Order does not alter or affect the applicability of the Federal Rules of Civil Procedure or Local Rules for the United States District Court for the Southern District of New York.
2. The production specifications set forth in this Stipulation and Order apply to Documents and ESI that is to be produced in the first instance in the above-captioned litigation. The parties will meet and confer concerning the applicability of this Stipulation and Order to any Documents to be reproduced in this action that were previously produced in another action or as part of a pre-complaint investigation.¹ The production specifications set forth in this Stipulation and Order do not apply to databases, data sources, logs, and other structured data except as described in paragraph L below.
3. "Actions" means collectively the actions centralized by the Judicial Panel on Multidistrict Litigation under the caption *In re Google Digital Advertising Antitrust Litig.*, No. 21-MD-3010 (PKC) (S.D.N.Y.), as well as any additional actions subsequently transferred and/or centralized with these Actions, including any related discovery, pretrial, trial, post-trial, or appellate proceedings. The term Action means an individual action within the Actions.

For the avoidance of doubt, "Actions" excludes pre-suit investigations by State Plaintiffs.

¹ The parties have met and conferred and agreed that responsive Investigation Materials (as defined in the Protective Order, ECF No. 297 at 5) need not be reproduced, but that parties shall retain the ability to make reasonable and proportionate requests pursuant to Appendix E (for higher quality images) and Appendix J (for links).

4. ESI Liaisons.

- a. Designation: Each party agrees to designate one or more ESI Liaisons within ten (10) days after entry of this ESI Protocol. Any party is free to change its designated ESI Liaisons by providing written notice to the other parties.
- b. Duties of ESI Liaisons: Each ESI Liaison will be prepared to participate in the resolution of any e-discovery disputes or ESI issues that may arise (or designate another person as primarily responsible), be knowledgeable about the party's eDiscovery efforts, have reasonable access to personnel most knowledgeable about the Party's electronic systems and capabilities in order to, as appropriate, explain those systems and answer relevant questions, including the location, nature, accessibility, format, collection, search methodologies, and production of ESI in this matter, and have reasonable access to those who are knowledgeable about the technical aspects of eDiscovery, including electronic document storage, organization, and format issues, and relevant information retrieval technology, including search methodology. The parties will rely on the liaisons, as needed, to confer about ESI and to help resolve disputes without court intervention.

II. PRESERVATION

1. Materials To Be Preserved. Each Party will continue its retention practices with regards to all Documents and ESI and will take reasonable and proportionate steps to preserve relevant and discoverable ESI in compliance with duties to preserve material under the Federal Rules of Evidence and the Federal Rules of Civil Procedure. Upon mutual agreement of the parties, a party will modify its retention practices to ensure the preservation of potentially responsive Documents and ESI.

2. To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the parties agree that:
 - a. Parties shall preserve non-duplicative relevant electronically stored information in their possession, custody, or control.
 - b. Subject to and without waiving any protection described above, the parties agree that:
 - i. The parties will endeavor to agree upon a date limitation for the preservation of ESI;
 - ii. The parties will endeavor to agree upon a list of the types of relevant ESI they believe should be preserved and the custodians for whom they believe relevant ESI should be preserved. The parties shall add or remove custodians as reasonably necessary.
3. The Court concludes that the following categories of ESI are not reasonably accessible in this litigation and orders that they need not be preserved, searched, collected, or reviewed. The parties will continue to meet and confer regarding any additional categories of information that are not reasonably accessible.
 - a. Back-up systems used for disaster recovery and tapes used for disaster recovery;
 - b. Individual user data subject to routine disposition required by privacy regulations;
 - c. Information from handsets, mobile devices, personal digital assistants, and tablets that is duplicative of information that resides in a reasonably accessible data source;
 - d. Logs of calls made from cellular phones;
 - e. Voicemail messages;
 - f. Slack, fragmented, or unallocated data accessible only by forensics;
 - g. Data stored in random access memory ("RAM"), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;

- h. Data in metadata fields that are frequently updated automatically, such as last-opened or last modified dates;
 - i. Ad log files concerning ads viewed outside the United States, Canada, the United Kingdom, Australia, New Zealand, and Ireland;²
 - j. Systems no longer in use that cannot be accessed as of the date the preservation obligation was triggered; and
 - k. Information created or copied during the routine, good-faith performance of processes for the deployment, maintenance, retirement, and/or disposition of computer equipment by the party that is duplicative of information that resides in a reasonably accessible data source.
4. Nothing in this Stipulation and Order prevents any party from asserting, in accordance with the Federal Rules of Civil Procedure, that other categories of Documents or ESI are not reasonably accessible.³
5. The parties agree to preserve ESI in such a way that it can be produced in a reasonably usable form in accordance with Federal Rule of Civil Procedure 34(b)(2)(E)(ii).
6. Preservation Does Not Affect Discoverability or Claims of Privilege. By preserving Documents and ESI for the purpose of this litigation, the Parties are not conceding that such material is discoverable, nor are they waiving any claim of privilege.

² The parties agree to meet and confer regarding a relevant and proportionate set of ad logs in these jurisdictions to be sampled and/or preserved. Nothing in this Order shall be construed as a concession regarding the relevance or irrelevance of any ad log files.

³ The parties have met and conferred and have been unable to reach agreement as to whether the following types of ESI are not reasonably accessible: (a) Online access data such as temporary or cache files, including internet history, web browser cache and cookie files, wherever located, (b) Server, system, or network logs; and (c) Dynamic fields of databases, dashboards, or log files.

III. COLLECTION AND REVIEW

1. The parties agree that in responding to an initial Fed. R. Civ. P. 34 request, they will meet and confer about methods to search ESI in order to identify ESI that is subject to production in discovery and filter out ESI that is not subject to discovery.
2. The parties will meet and confer in good faith regarding search terms or use of technology-assisted review or a similar tool (collectively "TAR") to identify responsive documents. In the event a party elects to use search terms, if a requesting party objects to the sufficiency of the producing party's terms, the requesting Party may propose modifications or a list of additional terms. The parties will meet and confer in good faith regarding any proposed changes. Any disputes over search terms that cannot be resolved between the parties during a meet and confer may be consequently raised with the Court.
3. Nothing in this Order may be construed or interpreted as precluding a producing party from performing a responsiveness review to determine if documents captured by search terms are in fact relevant to the requesting party's request. Nothing in this Order precludes a party from using TAR, or some other method to fulfill their document production obligations, provided that the party discloses to the other party the process used and complies with the meet and confer obligations outlined in this Order. However, a producing party that wishes to use TAR in combination with search terms must meet and confer with the receiving party before using this method to collect and review documents and prior to negotiation of search terms. Nothing may be construed or interpreted as precluding a producing party from performing a privilege review of documents determined to be relevant by any means. Further, nothing in this Order shall be construed or interpreted as requiring the production of all documents captured by any

search term or TAR if that document is in good faith and reasonably deemed not relevant to the requesting party's request or privileged.

4. Each party will use its best efforts to filter out common system files and application executable files by using a commercially reasonable hash identification process. Hash values that may be filtered out during this process are located in the National Software Reference Library ("NSRL") NIST hash set list.
5. De-Duplication. Each party is required to produce only a single copy of a responsive document. A producing party electing to deduplicate shall deduplicate across Custodians and at the family-level only (i.e., if there are identical child documents that have different parents, they are not duplicative, and an attachment to a document is not a duplicate of the same document maintained as a standalone document). Each party may de-duplicate responsive ESI (based on Source Hash, MD5 hash values, or other industry standard method) across Custodians. For emails with families, the hash value is generated based on the parent/child document grouping. To the extent that deduplication through hash values is not possible, the parties shall meet and confer to discuss any other proposed method of deduplication. A producing party must make reasonable effort to identify all agreed upon custodians who were in possession of any de-duplicated documents through an appropriate load file field such as All Custodians. Additionally, all BCC recipients whose names would have been included in the BCC metadata field, to the extent such metadata exists, but are excluded because of horizontal/global de-duplication, must be identified in the BCC metadata field specified in Appendix 1. In the event of rolling productions of documents or ESI, the producing party will, as needed, supplement the load files with updated All Custodian information, as well as BCC information to the

extent such metadata exists. Duplicate custodian information may be provided by a metadata overlay and will be provided by a producing party on an ongoing basis.

6. Email Threading. Production of a most inclusive email thread does not relieve the Producing Party of its obligation to produce responsive prior or lesser-included emails. No document shall be withheld from production solely on the basis that it is included in a produced more-inclusive email.⁴
7. Cooperation. The Parties agree to work together in good faith to resolve any differences that they may have over the Producing Party's use of search terms, TAR, or a combination of the search terms and TAR, or some other method, or for documents that cannot be searched electronically.
8. Filtering. If a producing party proposes to apply other filters to limit Documents and ESI that is collected for processing and review (e.g., filters that identify system files, non-user generated files, or zero-byte files), the producing party shall advise the requesting party and the requesting and producing parties shall meet and confer regarding such additional proposed filters.

Each Party shall use its institutional knowledge of how its ESI is stored and accessed in the ordinary course of business to identify responsive Documents. This institutional knowledge includes, but is not limited to, a Party's standard practices regarding the storage of ESI, its file organization structure, its usage of group ownership, group accounts, and shared network locations to manage or organize ESI.

⁴ This provision regarding email threading does not apply to Meta Platforms, Inc. ("Meta"). The only claims that have been asserted against Meta in this MDL relate to the Network Bidding Agreement, and discovery is currently stayed with respect to the Network Bidding Agreement. (*See* Dkt. No. 394 ¶ 3.) If Meta produces documents in this MDL, the Parties will meet and confer at that time regarding any use of email threading by Meta.

IV. PRODUCTION FORMAT

1. Subject to paragraph I.2 above, the parties agree to produce documents in the formats described in Appendix 1 to this Order. If particular documents warrant a different format, the parties will cooperate to arrange for the mutually acceptable production of such documents. The parties agree, to the extent practicable, not to materially degrade the searchability of the documents as part of the document production process.

V. PRIVILEGE LOGS

1. Any Producing Party will produce a privilege log within 45 days after each production. Except as provided otherwise below, for any Document withheld or redacted, the Producing Party will produce privilege logs in MS Excel (.xlsx) format.
2. If any member of a produced Document Family is withheld on grounds of privilege or work-product, the Producing Party shall produce a Bates stamped placeholder slipsheet that identifies the Document as withheld as privileged and shall identify the Document in the Privilege Log by the Bates number on the placeholder slipsheet.
3. Privilege logs shall be provided containing the following information, to the extent reasonably available:
 - a. A sequential number associated with each entry in the privilege log (Column A: row 1, row 2, row 3, etc.);
 - b. Where applicable, BegBates and Parent BegBates;
 - c. The Custodian or Custodial or Non-Custodial Data Source from which the Document was collected;
 - d. The name of each person who sent, authored, or otherwise prepared the Document;
 - e. The identity of each person designated as an addressee or copyee, including CC and BCC (copyees and blind copyees shall appear in separate fields);

- f. The date;
 - g. A description, pursuant to Federal Rule of Civil Procedure 26(b)(5)(A)(ii), of the contents of the withheld Document that, without revealing information that is itself privileged or protected, is sufficient to enable other Parties to understand the general subject matter of the Document and assess the basis of the claim of privilege or other protection from disclosure;
 - h. To the extent reasonably available, the name of the attorney(s) and legal organization who provided the legal advice at issue, from whom the legal advice at issue is requested, who directed the facilitation of the legal advice at issue, and/or who requested or prepared the Document;
 - i. The nature of the privilege or protection asserted (i.e., attorney-client privilege, work product doctrine).
4. If a Producing Party contends that all Documents of a particular type or category are privileged, they may request permission from and shall meet and confer with the Receiving Party to identify such Documents on a privilege log by category rather than individually. The Receiving Party shall consider any such request in good faith. The Producing Party's categorical privilege log entry must still provide the Requesting Party, and the Court if necessary, with information sufficient to evaluate the Producing Party's privilege claims.
5. A single document containing multiple email messages (i.e., in an email chain) may be logged as a single entry.
6. Each entry on a privilege log must indicate each person, group, or entity who was acting in a legal capacity with respect to that particular Document.

7. If the Producing Party contends that more than one basis for withholding applies to a single Document, all bases must be asserted in the privilege log.
8. Exclusions. To the extent any of the following Documents are privileged or otherwise protected from disclosure by Federal Rule of Civil Procedure 26(b)(3)-(4), they may be excluded from privilege logs:
 - a. Documents solely in the possession of outside counsel and their agents who represent a Party in any of these Actions;
 - b. Documents sent solely among a Party's outside counsel and their agents;
 - c. Documents that are non-discoverable or excluded from privilege log obligations under the Expert Stipulation;
 - d. Documents sent solely between counsel for the United States and counsel for any state;
 - e. Documents sent solely between counsel for any State and counsel for any other State;
 - f. Documents sent solely between outside counsel (and their agents) who represent a Party in any of these Actions and inside counsel for a Party;
 - g. Documents sent solely between or among (i) Defendants' counsel, or (ii) Plaintiffs' counsel.⁵
 - h. Documents sent solely among outside counsel and their agents who represent a Party in any of these Actions and the Parties they represent in these Actions, regarding the prosecution or defense of these Actions; and

⁵ Sub-paragraph V.8(g) shall only apply to communications occurring after December 16, 2020 (though no party waives any attorney-client or other privilege it may have over pre-December 16, 2020 communications). For purposes of this Order, "Plaintiffs' counsel" includes counsel for any Plaintiff in an Action and "Defendants' counsel" includes counsel for any Defendant in an Action.

- i. Documents the Producing Party may properly exclude from a privilege log pursuant to any subsequent order in the Actions.
9. If a Document contains both privileged and non-privileged communications, the non-privileged communications must be produced, either by separately producing a copy of the non-privileged communications embedded in the privileged communication, or by producing a copy of the entire communication string with the privileged portion(s) redacted. The redactions shall be narrowly applied so the Receiving Party has the ability to discern to the maximum extent practicable the privilege assertion within the Document and to view all non-privileged communications and material.
10. Redactions based on relevance or responsiveness or confidentiality are disallowed. For the avoidance of doubt, (a) to the extent that any Document contains or reflects Source Code, as defined by the Confidentiality Order entered on May 11, 2022, ECF No. 297, such Document will be governed by Appendix C of that Confidentiality Order, and (b) nothing in this Order prevents any party from redacting personal data and personally identifying numbers or sensitive information from produced documents, consistent with the requirements under Federal Rule of Civil Procedure 5.2 and Local Rules. The Parties do not waive any objections to the production, discoverability, admissibility, or confidentiality of Documents.
11. If a Document is produced with redactions, the redactions must not obscure any header information (e.g., from, to, subject, sent date) of any emails or other communications reflected in the Document, except to the extent that information is privileged.
12. A Party who, pursuant to a request under Federal Rule of Civil Procedure 34 or a non-party, pursuant to a request under Federal Rule of Civil Procedure 45, re-produces Documents from other matters, may produce privilege logs relating to that production in

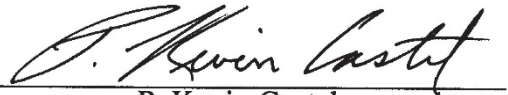
the manner they were produced in such other matters, so long as the privilege logs comply with Federal Rule of Civil Procedure 26(b)(5)(A). The party shall, however, reproduce these logs in Excel format upon request if reasonably possible to do so.

VI. MISCELLANEOUS PROVISIONS

1. Motions. The parties shall raise discovery disputes in accordance with the Individual Practices of Judge P. Kevin Castel. Discovery Disputes shall be brought on by letter and the parties shall comply with Local Civil Rule 37.2 unless otherwise ordered. A Discovery Dispute Letter to the Court shall contain the certification required under Rule 37(a)(1), Fed. R. Civ. P., and the full text of any discovery request and response or objection thereto, together with any case law support and any affidavits required to adjudicate the issue. The party from whom discovery is sought shall respond within four business days and shall include any case law support and any affidavits required to adjudicate the issue.
2. Costs of Document Production. Unless this Court orders otherwise for good cause shown, each party and non-party shall bear the costs of collecting, processing, reviewing, and producing its own documents.
3. Integration/Appendices. The following documents are incorporated herein by reference:
 - a. "Appendix 1" is a document describing the production format and fields to be included in the documents produced by each party.

SO ORDERED.

New York, NY
March 17, 2023


P. Kevin Castel
United States District Judge

APPENDIX 1: PRODUCTION FORMAT

A. Production Components. Except as otherwise provided below, ESI shall be produced in accordance with the following specifications:

1. An ASCII delimited data file (.DAT) with ASCII 020 for the comma character and ASCII 254 for the quote character and ASCII 174 for new line character, with all values in a multi-value field separated by a semi-colon ASCII 059 (with the use of commas and quotes as delimiters not acceptable using standard delimiters) and encoded in UTF-8;
2. An image load file (.OPT) that can be loaded into commercially acceptable production software (e.g. Concordance). The Image Load File shall contain the following comma-delimited fields: BEGBATES, VOLUME, IMAGE FILE PATH, DOCUMENT BREAK, FOLDER BREAK, BOX BREAK, PAGE COUNT;
3. TIFF images;
4. Document level .TXT files for all documents containing extracted full text or OCR text;
5. Parent-child relationships will be maintained in production and child files should be produced consecutively following parent files and shall be sequentially Bates stamped. The Producing Party shall ensure the metadata fields for BegAttach and EndAttach referenced in Part D of this Appendix A are accurately populated;
6. Document families must be produced, even if only the parent email or an attachment to an email is responsive, except (1) common system files and application executable files pursuant to paragraph III.4 above, and (2) documents that are withheld on the basis of attorney-client privilege or work product protection. For the avoidance of doubt, documents that are linked are not part of the same family for purposes of this Order. Linked documents are governed by Appendix J below.

If a particular document or category of documents warrants a different production format, for example if it is impractical to produce an entire document family for particular documents, the parties will cooperate in good faith to arrange for a mutually acceptable production format.

B. Production Media and Access Controls. Documents shall be produced through electronic means, such as secure file sharing methods (e.g. FTP) or on CD, DVD, flash drive or external hard drive ("Production Media"). Each piece of Production Media shall identify a production number corresponding to the production volume (e.g. "VOL001"). Each piece of Production Media shall also identify: (a) the producing party's name; (2) the production date; (3) the Bates Number range of the materials contained on the Production Media.

Nothing in this Order will preclude or impair any and all protections provided the parties by any Protective Order(s) agreed and entered into by the parties. Any data produced by the producing party must be protected in transit, in use, and at rest by all in receipt of such data. Parties will use best efforts to avoid the unnecessary copying or transmittal of produced documents. Any copies made of produced data must be kept on media or hardware employing whole-disk or folder level encryption or otherwise secured on information systems and networks in a manner consistent with the best practices for data protection. If questions arise, Parties will meet and confer to ensure security concerns are addressed prior to the exchange of any documents.

C. Data Load Files/Image Load Files. All production items will be provided with a delimited data file or "load file," which will include both an image cross-reference load file (such as an Opticon file) and a metadata (.dat) file with the metadata fields identified below on the document level to the extent available. Each TIFF in a production must be referenced in the corresponding image load file. The total number of documents referenced in a production's data load file should match the total number of designated document breaks in the image load file(s)

in the production. The total number of pages referenced in a production's image load file should match the total number of TIFF files in the production. All images must be assigned a unique Bates number that is sequential within a given document and across the production sets. The Bates numbers in the image load file must match the corresponding documents' beginning Bates numbers in the data load file. The total number of documents in a production should match the total number of records in the data load file. Load files shall not vary in format or structure within a production, or from one production to another.

D. Metadata Fields. With the exception of hard copy paper documents, which are separately addressed in paragraph M below, and except as provided in I.2, each of the metadata and coding fields set forth below that can be extracted shall be produced for each document, to the extent reasonably practicable. The parties are not obligated to populate manually any of the fields below if such fields cannot be extracted from a document, with the exception of the following: (a) BEGBATES, (b) ENDBATES, (c) BEGATTACH, (d) ENDATTACH, (e) CUSTODIAN, (f) ALLCUSTODIANS, (g) CONFIDENTIALITY, (h) REDACTIONS, (i) NATIVEFILEPATH, and (j) TEXTFILEPATH, which should be populated by the party or the party's vendor. The parties will make reasonable efforts to ensure that metadata fields automatically extracted from the documents correspond directly to the information that exists in the original documents.

| Field Name ⁶ | Field Description |
|-------------------------|-----------------------------------------------------------------|
| BEGBATES | Beginning Bates number as stamped on the production image |
| ENDBATES | Ending Bates number as stamped on the production image |
| BEGATTACH | First production Bates number of the first document in a family |

⁶ Field names can vary from system to system and even between different versions of systems. Thus, Parties are to be guided by these Field Names and Field Descriptions when identifying the metadata fields to be produced for a given document pursuant to this ESI Protocol Order.

| | |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ENDATTACH | Last production Bates number of the last document in a family |
| CUSTODIAN | Individual from whom the document originated |
| ALLCUSTODIAN(S) | Individual(s) whose documents de-duplicated out |
| CONFIDENTIALITY | Confidentiality designation assigned to document |
| MD5 HASH VALUE | MD5 hash value of document |
| SOURCE HASH VALUE | Google Drive Source hash value |
| AUTHOR | Any value populated in the Author field of the document and/or Google Drive properties (Edoc or attachment only) |
| DATECREATED | Date the document was created (format: MM/DD/YYYY) (Edoc or attachment only) |
| DATEMODIFIED | Date when document was last modified according to filesystem information (format: MM/DD/YYYY) (Edoc or attachment only) |
| FROM | The name and email address of the sender of the email |
| TO | All recipients that were included on the "To" line of the email |
| CC | All recipients that were included on the "CC" line of the email |
| BCC | All recipients that were included on the "BCC" line of the email |
| ATTACHMENT COUNT | Number of Attached Documents |
| ATTACHMENT NAME | File name of the document attachment or embedded document; associate with the parent/email which lists any and all filenames of the children/attachments delimited by a semicolon. The field would be populated for parent documents (not for the children) |
| ATTACHMENTID | The IDs of the documents that are attached to the produced document |
| COMPANIES | Globally populated field containing the name of producing party (not the law firm or vendor name). Not pulled from metadata. |
| DATE CREATED | Date the electronic file was created. Format: MM/DD/YYYY. |
| TIME CREATED | Time the electronic file was created (format: HH:MM:SS) |

| | |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DATERECEIVED | Date email was received (format: MM/DD/YYYY) |
| DATESENT | Date email was sent (format: MM/DD/YYYY) |
| DATESTART | Start date and time of calendar appointments, voice messages, chats, text message conversations. Format: MM/DD/YYYY HH:MM:SS (use 24 hour times, e.g., 13:32:00 for 1:32 pm); time zone indicators cannot be included. |
| DATEEND | End date and time of calendar appointments, voice messages, chats, text message conversations. Format: MM/DD/YYYY HH:MM:SS (use 24 hour times, e.g., 13:32:00 for 1:32 pm); time zone indicators cannot be included. |
| DRIVE COLLABORATORS | Users with access to edit a Google Drive document. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file . |
| DRIVE VIEWERS | Users with access to view a Google Drive Document. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file . |
| DOCUMENT TYPE | The file type for Google files. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file . |
| DOC ID | Google Drive unique identifier. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file . |
| DRIVE OTHERS | The accounts from a Google Drive query that have indirect access to the file. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file . |
| DRIVE SITES TITLE | Metadata included with Google Drive exports for sites, including the name of the page. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file . |
| DRIVE PUBLISHED URL | Metadata included with Google Drive exports for sites, including the web address of the published page. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file . |

| | |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | 59#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file. |
| DRIVE DOC PARENT ID | Metadata included with Google Drive exports for sites, including a unique identifier for the site. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file. |
| DRIVE SHARED DRIVE ID | The Google Drive identifier of the shared drive that contains the file. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file. |
| DRIVE CLIENT SIDE ENCRYPTED | In Google Drive, indicates the file was encrypted with Google Workspace Client-side encryption. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file. |
| DRIVE REVIEWS | Google Drive metadata regarding file approvals. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file. |
| DRIVE USER QUERY | The Google Drive query submitted by the Vault user that retrieved the files included in the export. See https://support.google.com/vault/answer/6099459#drivexml&zippy=%2Cfile-parameters-in-the-metadata-file. |
| DOC LINK | Metadata tying linked and linking documents, per Section J, below. |
| FILESIZE | The original file size of the produced document |
| ORIGINATING PATH | File path of the file as it resided in its original environment. For email, the full folder path of email within a mail store when collected, including file name; or full folder path of instant message or text message when collected including file name; or Hard Copy folder/binder title/label. Prepend with Custodian Name (sample: Smith, James-Inbox\Active). For other documents, the full absolute original path to the native, including original file name and root directory as they existed in their original environment, such that all information needed to locate the file is in the path. Prepend with recognizable Custodian Name; e.g. Smith, |

| | |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | James- C:\MyDocuments\Sales Info\ACME\2017-Monthly- Sales.xlsx |
| REDACTIONS | Indicate Yes if a document is redacted. If no leave blank. |
| NATIVE LINK | Native File Link (Native Files only) |
| EMAIL THREAD ID | Unique identification number that permits threading of email conversations. For instance, MS Outlook identification number ("PR CONVERSATION INDEX") is 22 bytes in length, followed by zero or more child blocks each 5 bytes in length, that facilitates use of email threading. (Microsoft application documents only) |
| TEXTFILEPATH | Path to extracted text/OCR file for document |
| EMAILSUBJECT | Subject Line of email |
| TIMESENT | Time email was sent |
| TIMEZONEUSED | Time zone used to standardize date/time during document processing |
| RECEIVETIME | Time email was received |
| FILENAME | File Name of the edoc or email |
| TITLE | Any value populated in Title field of the document properties |
| SUBJECT | Any value populated in the Subject field of the document properties |
| DOCEXT | File extension of the document |
| WITHHELD PLACHOLDER | To the extent a document is fully withheld (on the basis of privilege or otherwise), this field must be populated with a "Y". If not applicable leave blank. |
| TECHNICAL ISSUE PLACEHOLDER | To the extent a file is withheld on the basis of a technical issue, this field must be populated with a "Y". If not applicable leave blank. |
| VOLUMENAME | Unique production volume identifier applied (e.g., ABC001-001). |
| PAGECOUNT | For Documents produced in TIFF form, number of pages in the Document. For Documents produced in native, page count will be 1 (for placeholder) |

E. TIFFs. Documents that exist only in hard copy format shall be scanned and produced as TIFFs. Documents that exist as ESI shall be converted and produced as TIFFs, except as provided

below. The imaged data shall retain all attributes of the native or hard-copy file to the extent reasonably practicable. To the extent reasonably practicable, produced TIFF image will show all text and images that are visible in the form in which the electronic document was last saved, with the exception of redacted portions. Hidden content, tracked changes or edits, comments, notes, and other similar information, shall to the extent reasonably practicable, be produced in native or Microsoft-equivalent format, or be imaged so that such content is viewable on the image file. Where hidden content, tracked changes or edits, comments, notes, or other similar information is not readable in its produced format, a party that received the document may make reasonable requests that a more readable version, such as a native or Microsoft-equivalent version, be produced when helpful to interpret the contents of the relevant document. To the extent a response to discovery requires production of Document(s) accessible only through proprietary or enterprise software, the Parties shall meet and confer to finalize the appropriate production format. Unless excepted below, single page, black and white, Group IV TIFFs should be provided, at least 300 dots per inch (dpi) for all documents, with corresponding multi-page text and necessary load files. Each TIFF image shall be named according to a unique corresponding Bates number associated with the document. Each image shall be branded according to the Bates number and the agreed upon confidentiality designation. Original document orientation should be maintained (i.e., portrait to portrait and landscape to landscape). Documents that are difficult to render in TIFF because of technical issues, or any other documents that are impracticable to render in TIFF format, may be produced in their native format with a placeholder TIFF image stating "Document Produced Natively." A producing party retains the option to produce ESI in alternative formats if so agreed by the requesting party, which may include native format, or a combination of native and TIFF formats. For future productions of documents responsive to properly propounded requests issued pursuant to Fed. R. Civ. P. 34 and 45, the producing party

will make reasonable efforts to identify documents with readability issues in advance of production and, where issues are detected, to produce the document(s) in a more readable format (such as in native or Microsoft-equivalent form). The foregoing provisions of Appendix E do not apply to Investigation Materials (as defined in the governing Confidentiality Order, ECF No. 297) or other cloned discovery. To the extent that Investigation Materials or other cloned discovery contain documents responsive to properly propounded requests issued pursuant to Fed. R. Civ. P. 34 and 45 where the TIFF image is unreadable or has materially degraded the quality of the original, the producing party shall, when requested and where possible and proportionate, provide a higher quality TIFF image, or the native, Microsoft-equivalent, or original file. The provisions of this Appendix E apply to any type of document (including emails, presentations, spreadsheets, and other types of documents).

F. Color. A party that received a production may make reasonable requests that color images be produced where color is helpful to interpret the contents of the relevant document. The production of documents and/or ESI in color shall be made in single-page JPEG format (300 DPI). All requirements for productions stated in this ESI Protocol regarding productions in TIFF format apply to any productions of documents and/or ESI in color made in such an alternative format. Reasonable requests that a document be produced in color for the reasons set forth in this Paragraph will not be unreasonably denied by the producing party. If a producing party wishes to object, it may do so by responding in writing and setting forth its objection(s) to the production of the requested document in color.

G. Text Files. A single multi-page text file shall be provided for each document, and the filename should match its respective TIFF filename. When possible, the text of native files should be extracted directly from the native file. Text files will not contain the redacted portions of the documents. A commercially acceptable technology for optical character recognition "OCR" shall

be used for all scanned, hard copy documents and for documents with redactions. All Documents shall be produced with a link in the TextLink metadata field.

H. Native Files. Spreadsheets (e.g. MS Excel) will be produced in native format unless redacted. In the event spreadsheets require redactions, they shall be produced in Microsoft-equivalent format (.xls, .xlsx). If a Requesting Party reasonably determines that a redacted file is not reasonably usable, the Requesting Party and the Producing Party will discuss an alternative method to produce the file in a reasonably usable format. To the extent that they are produced in this action, audio, video, and multi-media files will be produced in native format. Native files shall be produced with a link in the NATIVEFILEPATH field, along with extracted text (where extracted text is available) and applicable metadata fields set forth in paragraph D above. A Bates numbered TIFF placeholder indicating that the document was provided in native format must accompany every native file.

I. Request for Other Native Files. Other than as specifically set forth above, a producing party need not produce documents in native format. If a party would like a particular document produced in native format and this ESI protocol does not require the production of that document in its native format, the party making such a request shall explain the reason for its request that the document be produced in its native format. The requesting party will provide a specific Bates range for documents it wishes to be produced in native format. The producing party need only produce such a document in native format if reasonably practicable. Any native files that are produced should be produced with a link in the Native Link field, along with all extracted text and applicable metadata fields set forth in Appendix D.

J. Linked Files and Collaborative Work Environments. For documents responsive to properly propounded requests issued pursuant to Fed. R. Civ. P. 34 or 45, the producing party shall conduct an automated search across all emails to be produced, where the producing party has

access to a tool capable of performing such an automated search, to identify any emails that contain links to another document and will conduct a reasonable search for the document corresponding with each identified link. A receiving party may also make reasonable and proportionate requests that the producing party conduct a reasonable search for relevant documents identified via hyperlinks. For each link identified by the receiving party, the producing party shall conduct a reasonable search for the document corresponding with the link. The producing party shall process and produce relevant documents corresponding with the links with reasonably available metadata. For documents produced pursuant to this Appendix J, the producing party is not required to conduct any further search of documents corresponding with the links. The provisions of this Appendix J apply to any type of document (including emails, presentations, spreadsheets, and other types of documents). For documents produced pursuant to this Appendix J, the producing party shall produce DOC LINK metadata as defined in Appendix D.

K. Confidentiality Designation. Responsive documents in TIFF format will be stamped with the appropriate confidentiality designations in accordance with the Protective Order entered in this matter. Each responsive document produced in native format will have its confidentiality designation identified in the filename of the native file and indicated on its corresponding TIFF placeholder.

L. Databases, Data Sources, Logs, and Other Structured Data. The parties shall meet and confer regarding the production format and scope of data contained in databases, data sources, and logs in order to ensure that any information produced is reasonably usable by the receiving party and that its production does not impose an undue burden on the producing party. To avoid doubt, information will be considered reasonably usable when produced in Parquet or other commonly utilized electronic formats, including CSV format, other character-delimited text format, Microsoft

Excel format, or Microsoft Access format. To the extent a party is constrained from producing responsive ESI because of a third-party license or because software necessary to view the ESI is hardware-dependent, the parties shall meet and confer in an attempt to reach an agreement on whether alternative methods exist to enable the requesting party to view the ESI.

M. Paper Documents. A producing party may make paper documents available for inspection and copying in accordance with Federal Rules of Civil Procedure 34 and 45 or, additionally or alternatively, scan and OCR paper documents. The following information shall be produced in the load file accompanying production of paper documents produced by scan and OCR to the extent reasonably practicable: (a) Beg Bates, (b) End Bates, (e) Custodian, (f) Confidentiality, (g) Redacted; (h) BegAttach (if applicable), (i) EndAttach (if applicable), (l) TextLink, (m) HashValue. Paper documents should be logically unitized for production to the extent reasonably practicable. Generally, when scanning paper documents for production, distinct documents shall not be merged into a single record and single documents shall not be split into multiple records. The parties will make reasonable efforts to unitize documents correctly. Where a document or a document group — such as folder, clipped bundle, or binder has an identification spine or other label, the information on the label shall be scanned and produced as the first page of the document or grouping to the extent reasonably practicable.

N. Date and Time. No party shall modify the date or time as contained in any original ESI. This provision does not prevent parties from deleting inaccurate date or time information that arises as an incident of collection or processing.

O. Time Zone. To the extent reasonably practicable, ESI items shall be processed using a consistent time zone and the time zone shall be disclosed to the requesting party.

P. Auto Date/Time Stamps. To the extent reasonably practicable, ESI items shall be processed so as to preserve the data/time shown in the document as it was last saved, not the date of collection or processing.

Q. Hidden Text. ESI items shall be processed, to the extent practicable, in a manner that preserves hidden columns or rows, hidden text and fields, worksheets, speaker notes, tracked changes, and comments.

R. Bates Numbers. Bates number must always: (1) contain no special characters or spaces;⁷ (2) for TIFF images, be sequential within a given Document; (3) identify the Producing Party; (4) maintain a constant length of nine numeric digits (including 0-padding) across the entire production; and (5) be unique across the entire production. Bates number must also maintain consistent numbering across a family of Documents. Bates numbers shall not be applied in a way that causes the text of the original Document to be obscured, deleted, or removed. If the Document contains a Bates number from a prior lawsuit, investigation, or production, the Producing Party shall avoid obscuring the previous Bates number or alternatively, shall provide a metadata overlay allowing the Requesting Party to identify the corresponding Bates number.

S. Compression Files. Compression or container file types (e.g., .CAB, .GZ, .RAR, .ZIP), shall, where possible, be decompressed to ensure that a compressed file within a compression or container file are decompressed into the lowest possible compression resulting in individual folders and/or files. Original compression files and container files need not be produced, provided that all Documents within the compression or container file are produced in accordance with the specifications of this Order.

T. Password Protected/Encrypted Files. To the extent Documents are password-protected or encrypted, the requesting party may make reasonable requests for the producing party to

⁷ For the avoidance of doubt, hyphens, dashes, and underscores are permitted and are not “special characters” within the meaning of this provision.

process such Documents for review. To facilitate the identification of such documents, the producing party shall provide a slip-sheet for any document that failed to process because it was password-protected or encrypted. Any slip-sheet produced pursuant to this Appendix T shall indicate that the reason the document failed to process was password-protection or encryption, as applicable. The producing party shall use reasonable efforts to produce such documents where possible and proportionate to do so. The parties shall meet and confer to resolve any disputes arising under this Appendix T.